Documentation

OpenScape Desk Phone IP
Phone Administration

Administrator Documentation

A31003-D3000-M100-01-76A9

Siemens Enterprise Communications
www.siemens-enterprise.com

SIEMENS

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG

Reference No.: A31003-D3000-M100-01-76A9

Siemens Enterprise Communications
www.siemens-enterprise.com

Contents

1 Overview

1.1 Important Notes

	Do not operate the equipment in environments where there is a danger of explosions.
	If Power over Ethernet (PoE) is not available: For safety reasons the phone should be operated using the supplied plug-in power unit.
	Use only original accessories from Siemens Enterprise Communications GmbH & Co. KG! Using other accessories may be dangerous, and will invalidate the warranty, extended manufacturer's liability and the CE mark.
	Never open the telephone or add-on equipment.
	Installation requirement for USA, Canada, Norway, Finland and Sweden: Connection to networks which use outside cables is prohibited. Only in-house networks are permitted.

	For USA and Canada only: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: • Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. Consult the dealer or an experienced radio/TV technician for help. This product is a UL Listed Accessory, I.T.E., in U.S.A. and Canada. This equipment also complies with the Part 68 of the FCC Rules and the Industrie Canada CS-03.

1.2 Maintenance Notes

	Do not perform maintenance work or servicing of the telephone in environments where there is a danger of explosions.
	Use only original accessories from Siemens Enterprise Communications GmbH & Co. KG. Using other accessories may be dangerous, and will invalidate the warranty and the CE mark.
	Never open the telephone or add-on equipment, e.g. a key module.

1.3 About the Manual

The instructions within this manual will help you in administering and maintaining the OpenScape Desk Phone. The instructions contain important information for safe and proper operation of the phones. Follow them carefully to avoid improper operation and get the most out of your multi-function telephone in a network environment.

This guide is intended for service providers and network administrators who administer VoIP services using the OpenScape Desk Phone and who have a fundamental understanding of VoIP, SIP, IP networking and telephony. The tasks described in this guide are not intended for end users.

These instructions are laid out in a user-oriented manner, which means that you are led through the functions of the OpenScape Desk Phone step by step, wherever expedient. For the users, a separate manual is provided.

You can find further information on the official Siemens Enterprise Communications website (http://www.siemens-enterprise.com) and on the Siemens Enterprise Wiki (http://wiki.siemens-enterprise.com).

1.4 Conventions for this Document

The terms for parameters and functions used in this document are derived from the web interface (WBM). In some cases, the phone's local menu uses shorter, less specific terms and abbreviations. In a few cases the terminologies differ in wording. If so, the local menu term is added with a preceding "/".

For the parameters described in this document, a WBM screenshot and the path in the local phone menu is provided.

This document describes the software version V3R2.

1.5 The OpenScape Desk Phone Family

1.5.1 OpenScape Desk Phone IP 35G

1	With the **Handset**, the user can pick up and conduct calls in the usual manner.
2	The **Display** provides intuitive support for telephone operation and allows the user to control the phone settings via the local User and Admin menu.
3	**The Fixed Function Keys (NOT re-programmable) provide access to frequently used telephony functions, as follows:** **Messages**: Provides access to the Call Log, allowing the user to view and manage the lists of **Missed Calls**, **Dialed Calls**, **Received Calls**, **Forwarded Calls** and to access and manage the **Voice Mail**. **Settings**: Provides access to the User and Admin menus for locally controlling the phone settings **Speaker**: Turns on/off the hands-free mode (speakerphone). **Headset**: Switches the audio sound to the headset or back from the headset to the handset speaker/speakerphone. **Vol. +** and **Vol. -**: Increases/decreases the speaker/headset and handset volume. **Mute**: Turns off/on the microphone during conversations. This feature is used to prevent the listening party from hearing what is being said at the calling party´s location or to prevent noise from being transmitted to all participants in conference calls.
4	With the **Navigation Keys**, the user/administrator can navigate through the various phone functions, applications, and configuration menus.
5	**The Fixed Function Keys (re-programmable via WBM or DLS) provide access to frequently used telephony functions, as follows:** **Transfer**: Transfers calls to other destinations. **Conference**: Provides access to the conferencing features. By default, pressing this key automatically seizes an outgoing line and turns on the hands-free mode. **Hold**: Places an ongoing call on hold or reconnects a held call.
6	The **Keypad** is used for entering phone numbers and text.
7	The **Free Programmable Keys** enable the user to customize the telephone in line with his/her personal needs by assigning individual phone numbers and functions. Preset default values: • Forward • Pick up • Do Not Disturb (DND)
8	Inbound calls are visually signaled via the **Alert Bar**. Waiting Voice Mail messages and Missed Calls are also signaled via the alert bar LED if the MWI LED and Missed call LED features are configured accordingly.

1.6 Administration Interfaces

You can configure the OpenScape Desk Phone by using any of the methods described in this chapter:

- via the Web Based Management (WBM) (see *1.6.1 Web-based Management (WBM)*;
  OR
- via the DSL (OpenScape Deployment Service) (see *1.6.2 DLS (OpenScape Deployment Service)*;
  OR
- via the Local Phone (see *Local Phone Menu*).

1.6.1 Web-based Management (WBM)

This method employs a web browser for communication with the phone via HTTPS. It is applicable for remote configuration of individual IP phones in your network. Direct access to the phone is not required.

INFO: To use this method, the phone must first obtain IP connectivity.

1.6.2 DLS (OpenScape Deployment Service)

The OpenScape Deployment Service (DLS) is an OpenScape Management application for administering phones and soft clients in both OpenScape and non-OpenScape networks. It has a Java-supported, web-based user interface which runs on an internet browser. For further information, please refer to the *OpenScape Deployment Service Administration Guide*.

1.6.3 Local Phone Menu

This method provides direct configuration of the OpenScape Desk Phone via the local phone menu. Direct access to the phone is required.

INFO: As long as the IP connection is not properly configured, you have to use this method to set up the phone.

2 Startup

2.1 Prerequisites

The OpenScape Desk Phone acts as an endpoint client on an IP telephony network, and has the following network requirements:

- An Ethernet connection to a network with SIP clients and servers.

> ***INFO:*** Only use switches in the LAN to which the OpenScape phone is connected. An operation at hubs can cause serious malfunctions in the hub and in the whole network.

- OpenScape Voice server.
- An FTP Server for file transfer, e. g. firmware, configuration data, application software.
- A DHCP (Dynamic Host Configuration Protocol) server (recommended).
- DLS (OpenScape Deployment Service) for advanced configuration and software deployment (recommended).

For additional information see the Wiki page *http://wiki.siemens-enterprise.com/wiki/IEEE_802.1x*

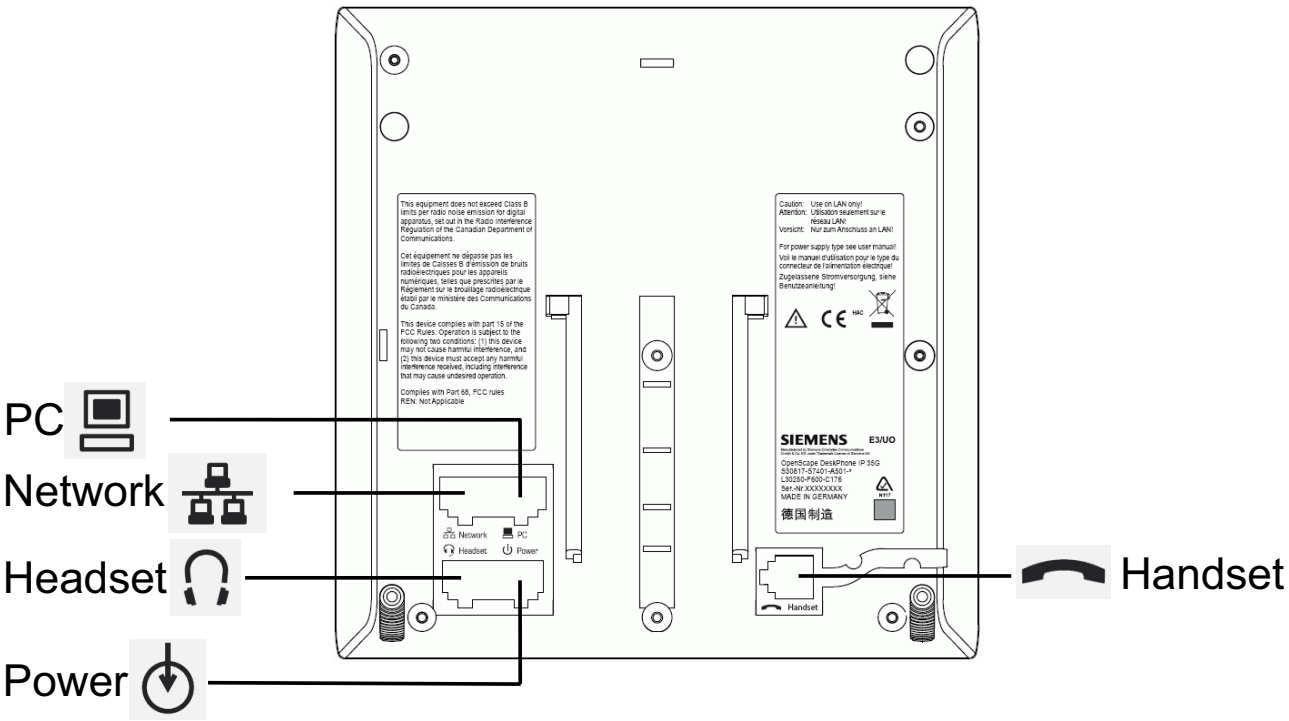
2.2 Assembling and Installing the Phone

2.2.1 Shipment

- Phone
- Handset
- Handset cable
- Subpackage:
  - Document "*Information and Important Operating Procedures*"
  - Emergency number sticker

2.2.2 Connectors at the Bottom Side

OpenScape Desk Phone IP 35G



2.2.3 Assembly

Step by Step

1) **Handset**

Insert the plug on the long end of the handset cable into the jack on the base of the telephone and press the cable into the groove provided for it. Next, insert the plug on the short end of the handset cable into the jack on the handset.

2) **Emergency Number Sticker**

Write your phone number and the emergency numbers for the fire and police departments on the included label and attach it to the telephone housing where applicable, e.g. underneath the handset.

2.2.4 How to Connect the Phone

Step by Step

1) Plug the LAN cable into the connector at the bottom side of the telephone and connect the cable to the LAN resp. switch.

a) If PoE (Power over Ethernet) is to be used, the PSE (Power Sourcing Equipment) must meet the IEEE 802.3af specification.

INFO: The required power supply for the OpenScape Desk Phone IP 35G must comply with the Power Consumption/Supply Class 2.

---

b) Only if Power over Ethernet (PoE) is **NOT** supported, you have to use the optional plug-in power supply:

INFO: The order no. for the plug-in power supply is region-specific:

- EU: C39280-Z4-C510
- UK: C39280-Z4-C512
- USA: C39280-Z4-C511

Plug the power supply unit into the mains. Connect the plug-in power supply unit to the jack at the bottom side of the phone.

2) If applicable, connect the following optional jacks:

- LAN connection to PC
- Headset (accessory)

2.3 Quick Start

This section describes a typical case: the setup of an OpenScape Desk Phone endpoint in an environment using a DHCP server and the web interface. For different scenarios, cross-references to the corresponding section of the administration chapter are given.

INFO: Alternatively, the DLS (OpenScape Deployment Service) administration tool can be used. Its Plug & Play functionality allows to provide the phone with configuration data by assigning

an existing data profile to the phone's MAC address or E.164 number. For further information, see the *Deployment Service Administration Manual*.

INFO: Any settings made by a DHCP server are not configurable by other configuration tools.

2.3.1 How to Access the Web Interface (WBM)

Prerequisites

- The phone´s IP address or URL is required for accessing the phone´s Web Interface via a web browser. By default, the phone will automatically search for a DHCP server on startup and try to obtain IP data and further configuration parameters from that central server.
- If no DHCP server is available in the IP network or if the DHCP parameter is disabled, the IP address, subnet mask and default gateway/route must be defined manually.
- To obtain the phone´s IP address, proceed as follows:

Step by Step

1) Access the local phone´s Admin menu as described in *Access via Local Phone*.

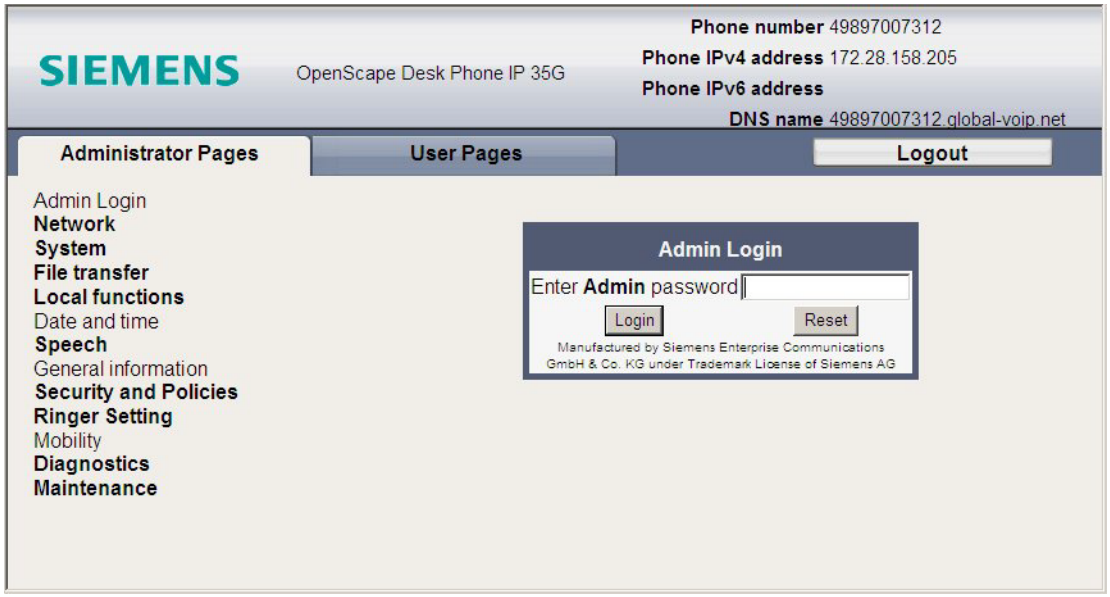
- If DHCP is **enabled** (default): In the **Admin** menu, navigate to **Network > IPv4 configuration > IP address**. The IP address is displayed.
- If DHCP is disabled or if no DHCP server is available in the IP network, the IP address, subnet mask and default gateway/route must be defined manually as described in *How to Manually Configure the Phone´s IP Address*.

2) Open your web browser (MS Internet Explorer or Mozilla Firefox) and enter the appropriate IP address or URL.

Example: `https://192.168.1.15` or `https://myphone.phones`

For configuring the phone's DNS name, please refer to *Terminal Hostname*.

If the browser displays a certificate notification, accept it. The start page of the web interface appears. In the upper right corner, the phone number, the phone's IP address, as well as the DNS name assigned to the phone are displayed. The left column contains the menu tree.



3) Click on the "Administrator Pages" tab. In the dialog box, enter the admin password. **The default password is 123456**.

4) The administration main page opens. The left column contains the menu tree. If you click on an item which is printed in normal style, the corresponding dialog opens in the center of the page. If you click on an item printed in bold letters, a sub-menu opens to the right of the main menu.

2.3.2 How to Set the Terminal Number

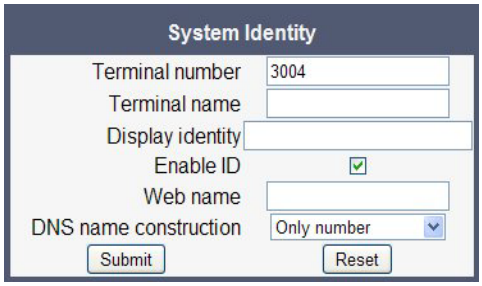
Prerequisites

- If the user and administrator menus are needed in the course of setup, the terminal number, which by default is identical with the phone number, must be configured first. When the phone is in delivery status, the terminal number input form is presented to the user/administrator right after booting, unless the Plug&Play facility of the DLS is used. For further information about this setting, please refer to *Terminal Identity*. With the WBM, the terminal number is configured as follows:

Step by Step

1) Log on as administrator to the WBM by entering the access data for your phone.

2) In the Administrator menu (left column), select System > System Identity to open the "System Identity" dialog. Enter the terminal number, i. e. the SIP name / phone number. For further information, please refer to *Terminal Identity*.



2.3.3 Basic Network Configuration

For basic functionality, DHCP must provide the following parameters:

- IP Address: IP Address for the phone.
- Subnet Mask (option #1): Subnet mask of the phone.
- Default Route (option #3 "Router"): IP Address of the default gateway which is used for connections beyond the subnet.
- DNS IP Addresses (option #6 "Domain Server"): IP Addresses of the primary and secondary DNS servers.

If no DHCP server is present, see *IP Address - Manual Configuration* for IP address and subnet mask, and *Default Route/Gateway* for the default route.

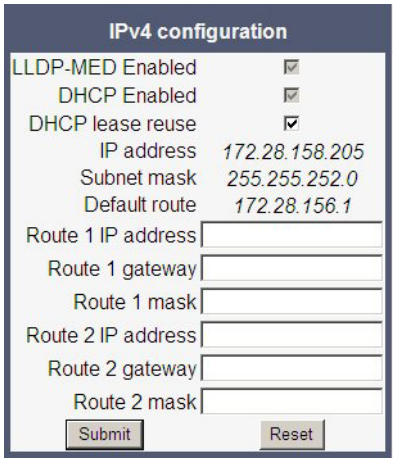
2.3.4 DHCP Resilience

Prerequisites

- It is possible to sustain network connectivity in case of DHCP server failure. If **DHCP lease reuse** is activated, the phone will keep its DHCP-based IP address even if the lease expires. To prevent address conflicts, the phone will send ARP requests in 5 second intervals. Additionally, it will send discovery messages periodically to obtain a new DHCP lease.

Step by Step

› In the left column, select **Network > IPv4 configuration** to open the "System Identity" dialog. Select the check box to enable **DHCP lease reuse**.



2.3.5 Date and Time / SNTP

An SNTP (Simple Network Time Protocol) server provides the current date and time for network clients. The IP address of an SNTP server can be given by DHCP.

In order to provide the correct time, it is required to give the time zone offset, i.e. the shift in hours to be added to the UTC time provided by the SNTP server.

The following DHCP options are required:

- SNTP IP Address (option #42 "NTP Servers"): IP Address or hostname of the SNTP server to be used by the phone.
- Time zone offset (option #2 "Time Offset"): Offset in seconds in relationship to the UTC time provided by the SNTP server.
  For manual configuration of date and time see *3.5.4 Date and Time*.

2.3.6 SIP Server Address

The IP Address or hostname of the SIP server can be provided by DHCP.

The option's name and code are as follows:

- **option #120 "SIP Servers DHCP Option"**
  For manual configuration of the SIP server address see *SIP Addresses*.

2.3.7 Extended Network Configuration

To have constant access to other subnets, you can enter a total of two more network destinations. For each further domain/subnet you wish to use, first the IP address for the destination, and then that of the router must be given. The option's name and code are as follows:

- **option #33 "Static Routing Table"**
  For manual configuration of specific/static routing see *Specific IP Routing*.
- Also the DNS domain wherein the phone is located can be specified by DHCP. The option's name and code are as follows:
  option #15 "Domain Name"
  For manual configuration of the DNS domain name see *DNS Domain Name*.

2.3.8 Vendor Specific: VLAN Discovery and DLS Address

INFO: The VLAN ID can also be configured by LLDP-MED (see *Automatic VLAN discovery using LLDP-MED*).

If the phone is to be located in a VLAN (Virtual LAN), a VLAN ID must be assigned. In case the VLAN shall be provided by DHCP, VLAN Discovery must be set to "DHCP" (see *Automatic VLAN discovery using DHCP*).

If a DLS (Deployment Service) server is in use, its IP address must be provided. It is recommended to configure the DLS server address by DCHP, as this method enables full Plug & Play: having received the DLS address from DHCP, the phone will contact the DLS during start-up. Provided that the DLS is configured appropriately, it will send all necessary configuration data to the phone. Additionally, this method is relevant to security, as it ensures the authenticity of the DLS server.

For manual configuration of the DLS server address see *Configuration & Update Service (DLS)*.

For the configuration of vendor-specific settings by DHCP, there are two alternative methods:

- the use of a vendor class - see *How to Use a Vendor Class*,

or

- the use of DHCP option 43 - see *How to Use Option #43 "Vendor Specific"*.

2.3.8.1 How to Use a Vendor Class

Prerequisites

- It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients.
- In the following, the configuration of vendor classes is explained both for a Windows DHCP Server and for Unix/Linux.

Example: Configuration of the Windows DHCP Server

INFO: For DHCP servers on a pre-SP2 Windows 2003 Server.

Windows 2003 Server contains a bug that prevents you from using the DHCP console to create an option with the ID 1 for a user-defined vendor class. Instead, this entry must be created with the netsh tool in the command line (DOS shell).

You can use the following command to set the required option (without error message), so that it will appear in the DHCP console afterwards:

netsh dhcp server add optiondef 1 "Optipoint element 001" STRING 0 vendor=OptiIpPhone comment="Tag 001 for Optipoint"

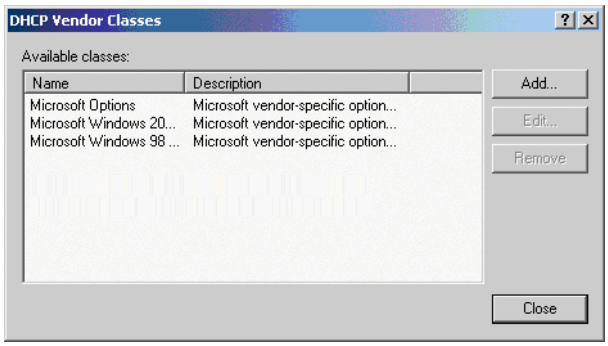
The value "Siemens" for optiPoint Element 1 can then be re-assigned using the DHCP console.

This error was corrected in Windows 2003 Server SP2.

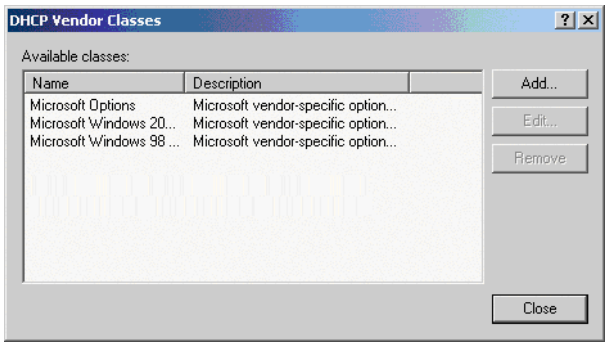
Step by Step

1) In the Windows Start menu, select **Start > Programs > Administrative Tools > DHCP**.

2) In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.

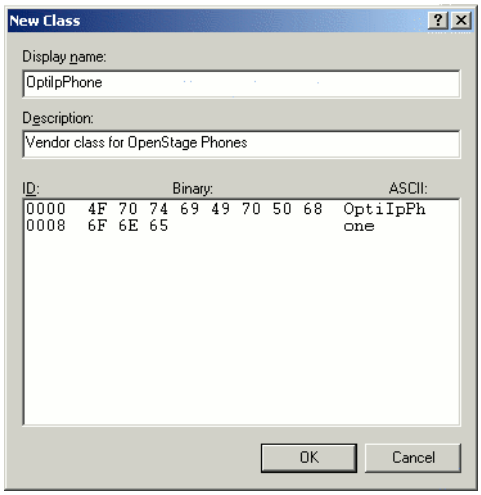


A dialog opens with a list of the classes that are already available.

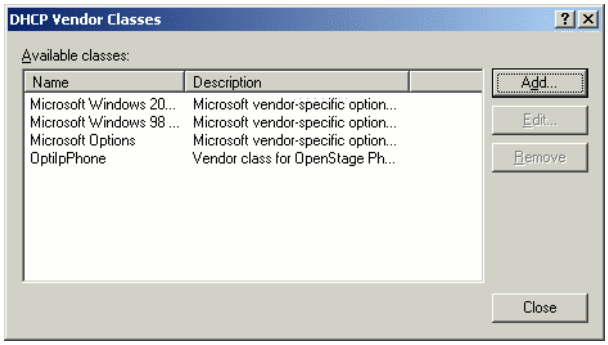


3) Press **Add...** to define a new *vendor class.*

4) Enter "**OptiIpPhone" as Display name** and give a description of this class. Provide the class name proper by setting the cursor underneath ASCII and typing "**OptiIpPhone".** The binary value is displayed simultaneously.

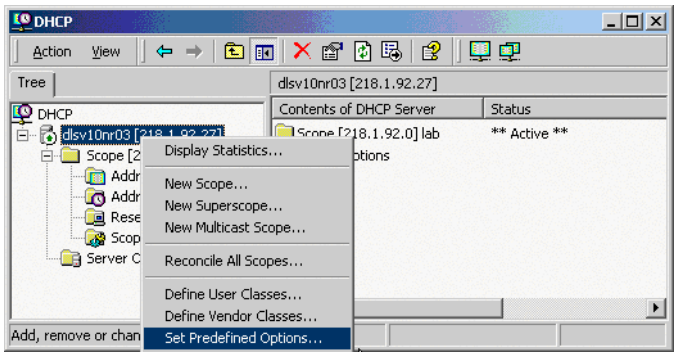


5) Click **OK** to apply the changes. The new vendor class now appears in the list:

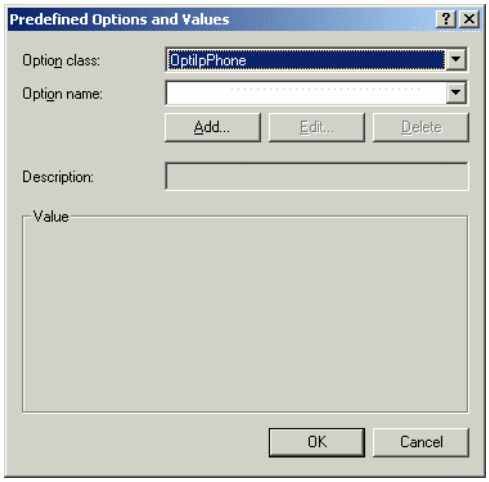


6) Exit the window with **Close**.

7) In the DHCP console menu, right-click the DHCP server in question and select **Set Predefined Options** from the context menu.



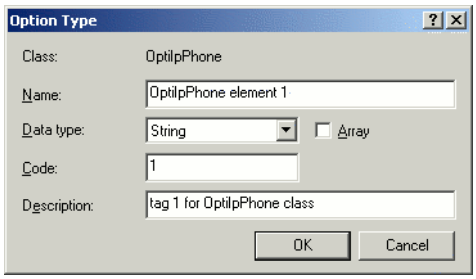
8) In the dialog, select the previously defined OptiIpPhone class and click on **Add...** to add a new option. (If the workaround for a pre-SP2 Windows 2003 Server has been applied, the first option will be there already.)



9) In the following dialog, specify the option type as follows. (If the workaround for a pre-SP2 Windows 2003 Server has been applied, the option type dialog will be skipped for the first option.)

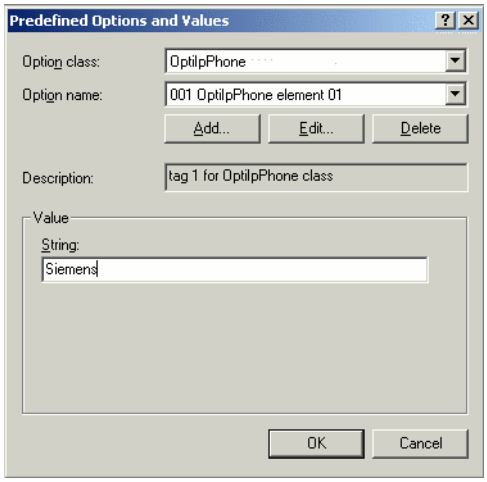
- **Name**: Free text, e. g. "OptiIpPhone element 01".
- **Data type**: "String".

- **Code**: "1".
- **Description**: Free text, e. g. "tag 1 for OptiIpPhone class".



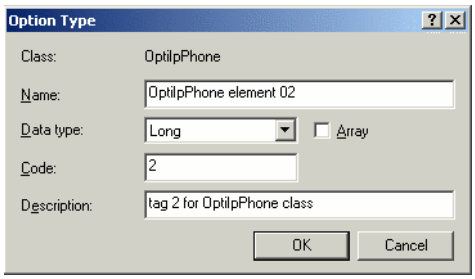
Click **OK** to return to the previous window.

10) The newly created option is displayed now. Enter "`Siemens`" in the **Value** field.



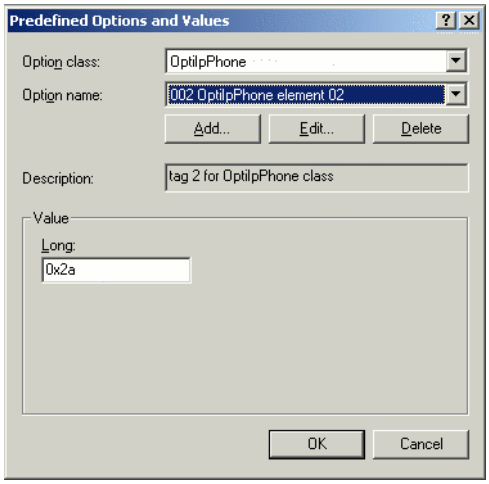
11) If the VLAN is to be provided by DHCP: Repeat step 7 and 8, and then specify the option type as follows. If you want to proceed to the configuration of the DLS address, continue with step 13.

- **Name**: Free text, e. g. "OptiIpPhone element 02"
- **Data type**: "Long"
- **Code**: "2"
- **Description**: Free text, e. g. "tag 2 for OptiIpPhone class".



Click **OK** to return to the previous window.

12) The newly created option is displayed now. Enter the VLAN ID as a hexadecimal number in the **Value** field. In the example, the VLAN ID is 42 (Hex: 0x2A).



If you do not intend to configure the DLS address, click **OK** and continue with step 15.

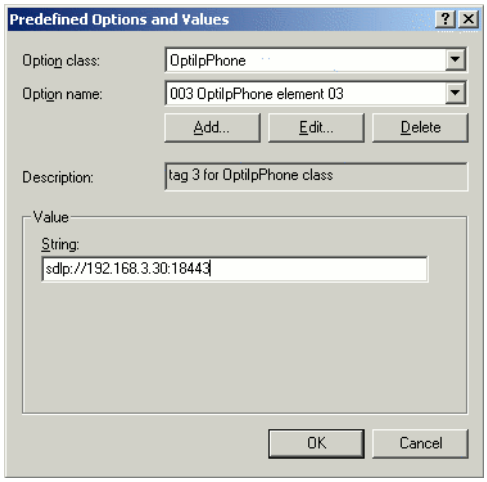
13) If the DLS address is to be provided by DHCP: Repeat step 7 and 8, and then specify the option type as follows.

- **Name**: Free text, e. g. "OptiIpPhone element 03".
- **Data type**: "String".
- **Code**: "3"
- **Description**: Free text, e. g. "tag 3 for OptiIpPhone class".

Click **OK** to return to the previous window.

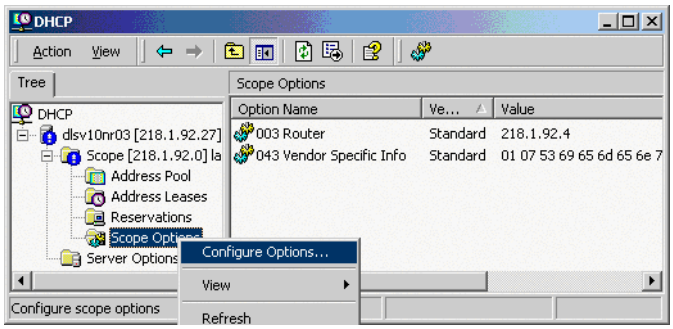
14) The newly created option is displayed now. Enter the DLS address in the **Value** field, using the following format:

<PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER> In the example, the DLS address is "sdlp://192.168.3.30:18443".

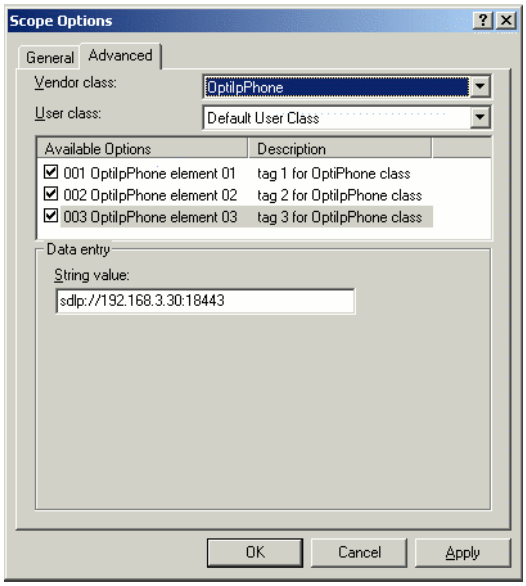


Click **OK**.

15) To define a scope, select the DHCP server in question, and then **Scope**, and right-click **Scope Options**. Select **Configure Options**... in the context menu.

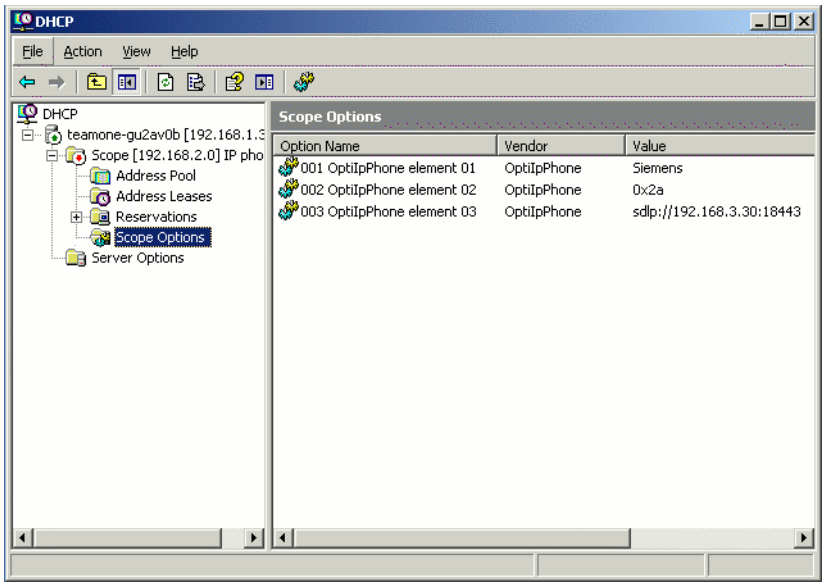


16) Select the **Advanced** tab. Under **Vendor class**, select the class that you previously defined (**OptiIpPhone**) and, under **User class**, select **Default User Class**.



Activate the check boxes for the options that you want to assign to the scope (in the example, **001**, **002**, and **003**). Click **OK**.

17) The DHCP console now shows the information that will be transmitted to the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **OptiIpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.



2.3.8.2 Setup using a DHCP Server on Unix/Linux

The following snippet from a DHCP configuration file (usually dhcpd.conf) shows how to set up a configuration using a vendor class and the "vendor-encapsulated-options" option.

```
class "OptiIpPhone" {
   option vendor-encapsulated-options
   # The vendor encapsulated options consist of hexadecimal values
for the option number (for instance, 01), the length of the value
(for in-stance, 07), and the value (for instance,
53:69:65:6D:65:6E:73). The options can be written in separate
lines; the last option must be followed by a ';' instead of a ':'.
   # Tag/Option #1: Vendor must be "Siemens"
   #1  7  S  i e m e n s
    01:07:53:69:65:6D:65:6E:73:
   # Tag/Option #2: VLAN ID
   # 2  4  0  0  0 10
    02:04:00:00:00:0A;
   # Tag/Option #3: DLS IP Address (here: sdlp://
192.168.3.30:18443)
   # 3 25 s  d  l  p  :  / /  1  9  2  .  1  6  8  .  3  .
(...etc.)
    03:19:73:64:6C:70:3A:2F:2F:31:39:32:2E:31:36:38:2E:33:2E:33:3
0: 3A:31:38:34:34:33;
   match if substring (option vendor-class-identifier, 0, 11) =
   "OptiIpPhone";
}
```

2.3.8.3 How to Use Option #43 "Vendor Specific"

Alternatively, option #43 can be used for setting up the VLAN ID and DLS address. The following tags are used:

- Tag 1: Vendor name
- Tag 2: VLAN ID
- Tag 3: DLS address

Optionally, the DLS address can be given in an alternative way:

- Tag 4: DLS host name

The Vendor name tag is coded as follows (the first line indicates the ASCII values, the second line contains the hexadecimal values):

Code	Length	Vendor name						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

The following example shows a VLAN ID with the decimal value "10". Providing:

Code	Length	VLAN ID			
2	4	0	0	1	0
02	04	00	00	00	0A

For manual configuration of the VLAN ID see *Manual Configuration of a VLAN ID*.

The DLS IP address tag consists of the protocol prefix "sdlp://", the IP address of the DLS server, and the DLS port number, which is "18443" by default. The following example illustrates the syntax:

Code	Length	DLS IP address																								
3	25	s	d	l	p	:	/	/	1	9	2	.	1	6	8	.	3	.	3	0	:	1	8	4	4	3
03	19	73	64	6C	70	3A	2F	2F	31	39	32	2E	31	36	38	2E	33	2E	33	30	3A	31	38	34	34	33

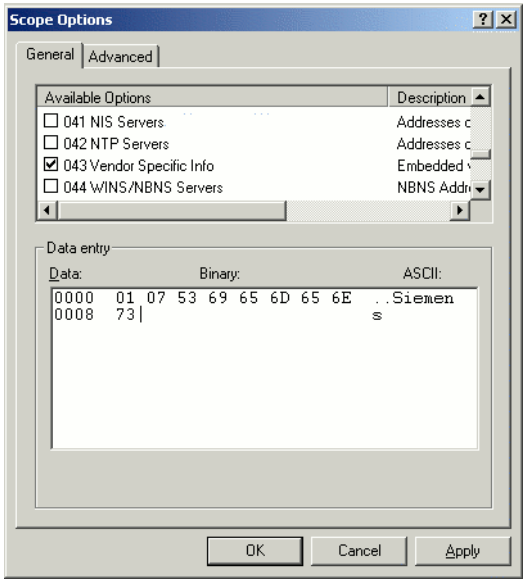
Example: Setup Using the Windows DHCP Server

Step by Step

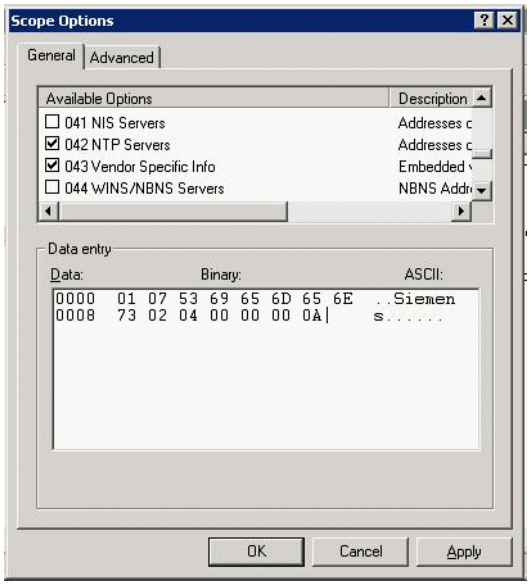
1) In the Windows Start menu, select **Start > Programs > Administrative Tools > DHCP**.

2) Select the DHCP server and the scope. Choose **Configure Options** in the context menu using the right mouse button.

3) Enter tag 1, that is the vendor tag. The value has to be "Siemens".



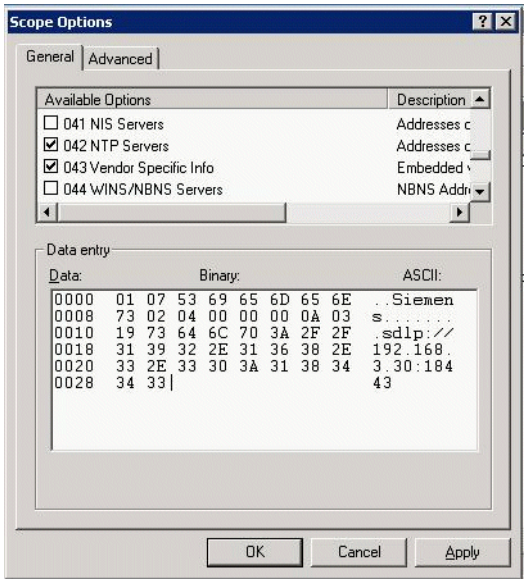
4) If the VLAN ID is to be provided by DHCP: Enter the hexadecimal value in **Data entry**. In the example, the VLAN ID is 10 (Hex: 0A).



5) If the DLS address is to be provided by DHCP: Enter the DLS address in the **Value** field, using the following format: <PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>

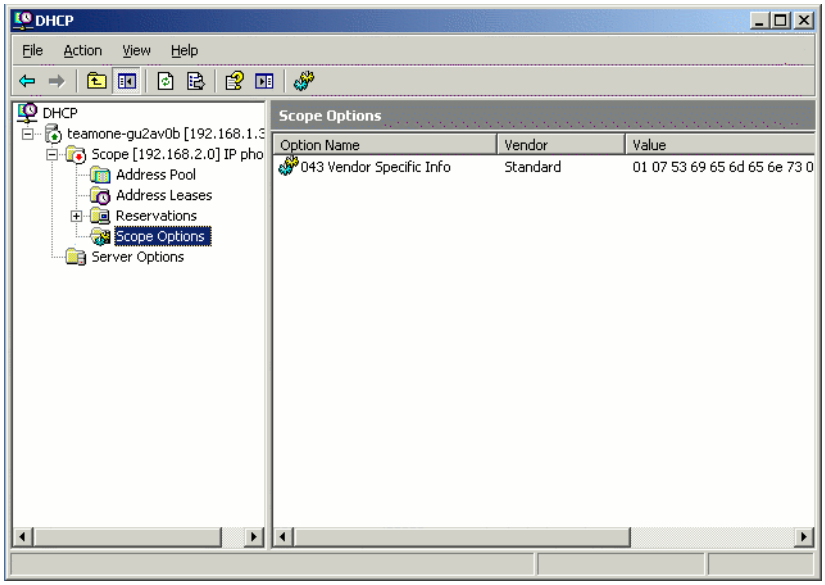
> ***INFO:*** For ensuring proper functionality, the port number should not be followed by any character.

In the example, the DLS address is "sdlp://192.168.3.30:18443". Note that the screenshot also shows the VLAN ID described in step 4.



Click **OK**.

6) The DHCP console now shows the information that will be transmitted to the corresponding workpoints.



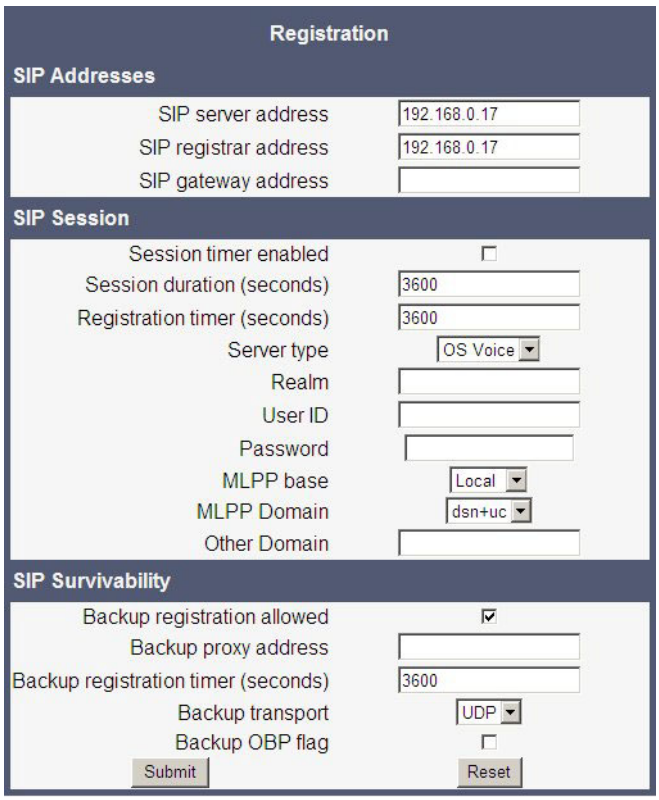
2.3.9 How to Register at OpenScape Voice

Prerequisites

- For registration at the OpenScape Voice server, a SIP user ID (and password, if required, depending on the SIP Server configuration) must be provided by the phone. The following procedure describes the configuration using the web interface (see *2.3.1 How to Access the Web Interface (WBM)*; if the web interface is not accessible, please refer to *3.5.6 SIP Registration*) for configuration via the local menu.

Step by Step

1) In the administration menu, select **System > Registration**. The **Registration** dialog opens.



2) Make sure that **SIP server address** and **SIP registrar address** contain the IP address of your OpenScape Voice server. If not provided by DHCP or DLS, enter the appropriate values. If the phone is to register with a gateway, enter the appropriate **SIP Gateway address**.

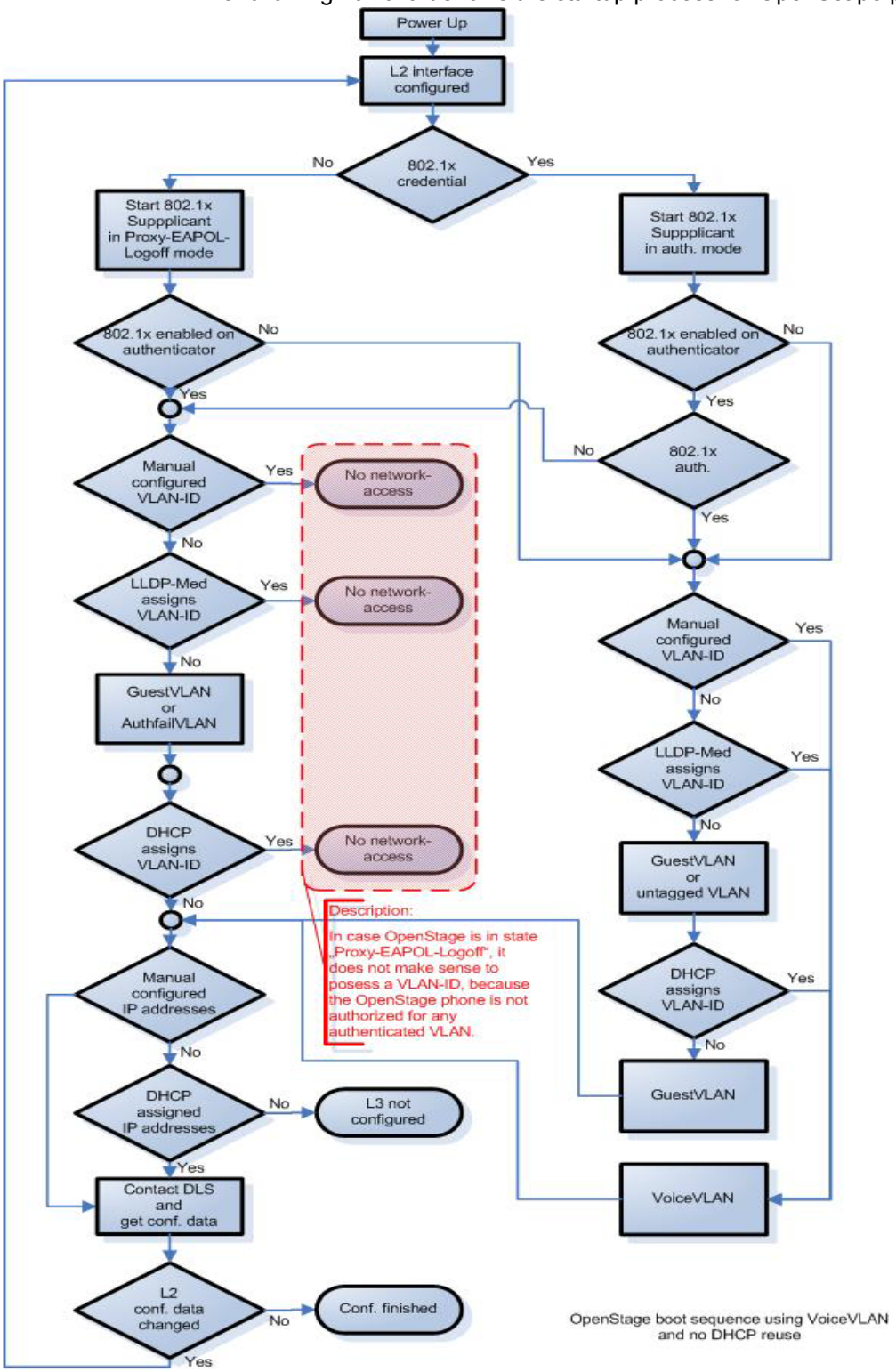
3) In the **Server type** field, select "OS Voice".

4) In **Realm**, enter the SIP realm the targeted user/password combination refers to. This setting depends on the configuration of the OpenScape Voice server.

5) In the **User ID** and **Password** fields, enter the user name/password combination for the phone. This setting depends on the configuration of the OpenScape Voice server.

2.4 Startup Procedure

The following flowchart shows the startup process for OpenScape phones:



2.5 Cloud Deployment (V3 R1)

This chapter describes how a phone progresses through the cloud deployment process from factory start-up until the cloud service provider considers it to be ready for use by its user.

The phone determines that a cloud deployment process is to be used based on the IP settings it receives from the DHCP at the customer site. The SEN Redirect server[1] requires a code to determine which cloud service provider is responsible for the phone. The code is provided as part of a pin supplied from the cloud organisation to the user. When the user enters the pin at the phone the SEN Redirect server redirects the phone to a DLS-WPI based management system operated by the cloud service provider. This management system completes the configuration of the phone with all the information required for it to be usable and may also customise the phone for the cloud service provider's 'house' style.

2.5.1 Process of Cloud Deployment

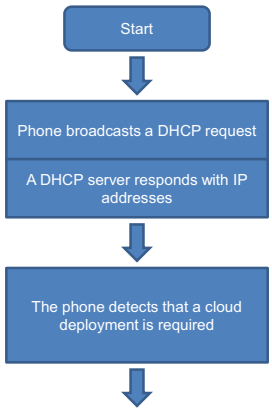
The following flow chart shows the way from a factory start-up to a user prepared OpenScape Desk Phone, deployed by a relevant DLS-WPI based management system.

Preconditions:

- Phone is not running
- Phone is set to factory default values
- The phone has a LAN connection

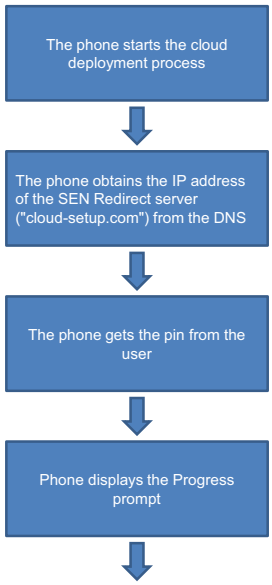
1. The address for the SEN Redirect server is hardcoded as "cloud-setup.com"

- The LAN connection provides access to the public internet



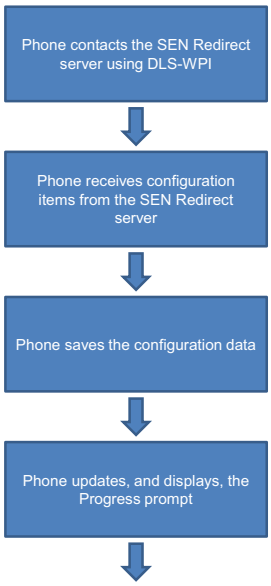
The phone has all the information that it needs to contact a DNS server.
A DLS address is not provided.

DHCP is available; IP address allocated to the phone;
DNS address is available; Subnet mask is available;
Router address is available; No DLS address available;
No SIP addresses available



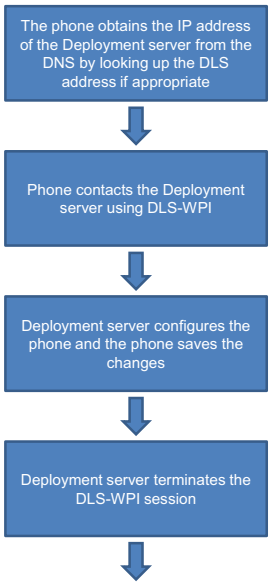
The phone is locked so that the mode keys & FPKs etc. cannot be used.

The user enters the pin and presses **OK.**
The phone verifies that the pin is valid.
The user has the option to **cancel** the process (see chapter 2, “Aborting Cloud Deployment process by User”.



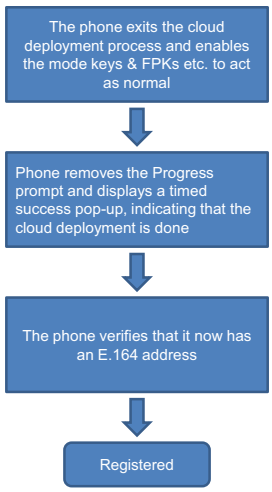
- DLS address (set to the name of the Deployment server)
- Language optional)
- DLS port (optional)

If the language is changed, then the display is updated



The stored DLS address is not changed by the result of the DNS lookup

The hash of the pin is provided as an Inventory item to the Deployment server



2.5.2 Aborting Cloud Deployment Process by User

The phone detects that a cloud deployment is required and starts the cloud deployment process. The phone expects the input of the PIN by the user. At this point the user has the option to cancel the process with **Cancel**. If the user confirms his decision, the deployment process is aborted.

2.5.3 Re-trigger Cloud Deployment

Cloud deployment may be restarted by triggering a Factory reset:

The DLS-WPI requests a restart to factory defaults of the phone. The phone restart should then trigger the cloud deployment process if the conditions in *Cloud Deployment* are still met.

2.5.4 Deployment errors

During deployment the display will always show deployment specific information. A persistent warning popup displays the information that will be shown in an idle screen error after deployment failed.

Code	Priority	Cause
AU	1	Abandoned by user. Occurs when the pin prompt is dismissed.
RS	1	Unable to get the address for the SEN Redirect server. DNS lookup failed.
RN	3	Unable to establish contact with SEN Redirect server – no reply.
RR	2	Unable to establish contact with SEN Redirect server – refused.
DS	1	Unable to get the address for the Deployment server. DNS lookup failed.
DN	3	Unable to establish contact with Deployment server – no reply.
DR	2	Unable to establish contact with Deployment server – refused.

3 Administration

This chapter describes the configuration of every parameter available on the OpenScape Desk Phones. For access via the local phone menu, see the subsequent description; for access via the web interface (WBM), please refer to *How to Access the Web Interface (WBM)*.

3.1 Access via Local Phone

Prerequisites

- The data entered in input fields is parsed and controlled by the phone.

Step by Step

1) Access the Administration Menu

Press the **Settings**, **Up Arrow** or **Down Arrow** and **OK** keys consecutively to select the **Admin** menu.

2) When the **Admin** menu is active, you will be prompted to enter the administrator password.

The default admin password is 123456. It is highly recommended to change the password (see *Password*) after your first login.

For entering passwords with non-numeric characters, please consider the following:

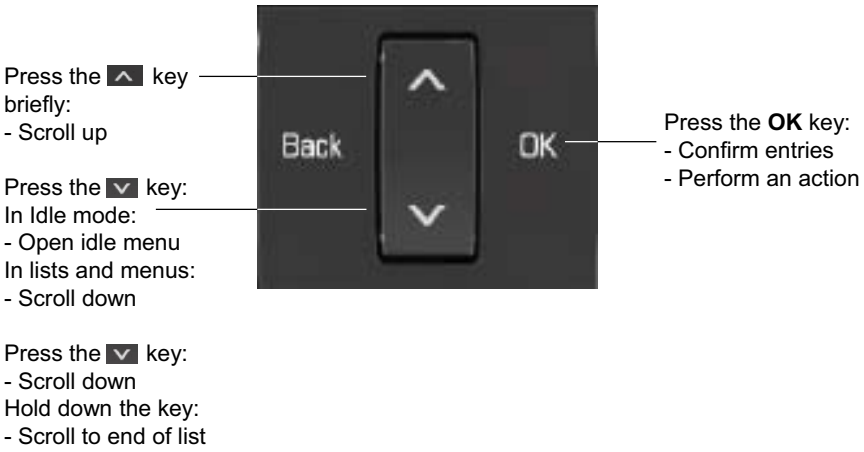
By default, password entry is in numeric mode. For changing the mode, press the **#** key once or repeatedly, depending on the desired character. The **#** key cycles through the input modes as follows:

(Abc) > (abc) > (123) > (HEX) > (ABC) > back to start.

Usable characters are 0-9 A-Z a-z .*#,?!'+-()@/:_

3) Navigate within the Administration Menu

Use the navigation keys to navigate and execute administrative actions in the administration menu.



4) Select a parameter.

If a parameter is set by choosing a value from a selective list, an arrow symbol appears in the parameter field that has the focus. Press the **OK** key to enter the selective list. Use the **Up Arrow** and **Down Arrow** keys to scroll up and down in the selection list. To select a list entry, press the **OK** key.

5) Enter the parameter value.

For selecting numbers and characters, you can use special keys. See the following table:

Key	Function
*	Switch to punctuation and special characters.
#	Toggle between lowercase characters, uppercase characters, and digits in the following order: (Abc) > (abc) > (123) > (HEX) > (ABC) > back to start.

With the OpenScape Desk Phone IP 35G, use the keypad for entering parameter values. Use the navigation keys to navigate and execute administrative actions in the Administration menu.

6) Save and exit the menu.

When you are done, select **Save & exit** and press the **OK** key.

3.2 LAN Settings

3.2.1 LAN Port Settings

The OpenScape Desk Phone IP 35G provides an integrated switch which connects the LAN, the phone itself and a PC port. By default, the switch will auto negotiate transfer rate (10/100 Mb/s, 1000 Mb/s with OpenScape Desk Phone IP 35G) and duplex method (full or half duplex) with whatever equipment is connected. Optionally, the required transfer rate and duplex mode can be specified manually using the LAN port speed parameter.

> ***INFO:*** In the default configuration, the LAN port supports automatic detection of cable configuration (pass through or crossover cable) and will reconfigure itself as needed to connect to the network.

The PC Ethernet port (default setting: **Disabled**) is controlled by the PC port mode parameter. If set to "Disabled", the PC port is inactive; if set to "Enabled", it is active. If set to "Mirror", the data traffic at the LAN port is mirrored at the PC port. This setting is for diagnostic purposes. If, for instance, a PC running Ethereal/Wireshark is connected to the PC port, all network activities at the phone's LAN port can be captured.

> ***INFO:*** Removing the power from the phone, or a phone reset/ reboot will result in the temporary loss of the network connection to the PC port.

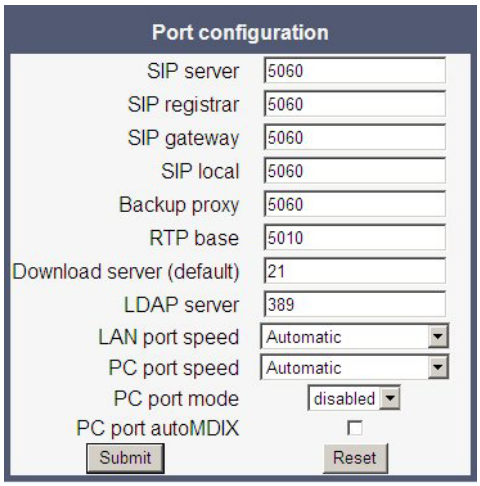
When PC port autoMDIX is enabled, the switch determines automatically whether a regular MDI connector or a MDI-X (crossover) connector is needed, and configures the connector accordingly.

Data required

- LAN port speed / LAN port type: Settings for the ethernet port connected to a LAN switch. Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex". Default: "Automatic"
- PC port speed / PC port type: Settings for the ethernet port connected to a PC. Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex". Default: "Automatic"
- PC port mode / PC port status: Controls the PC port. Value range: "disabled", "enabled", "mirror". Default: "disabled"
- PC port autoMDIX: Switches between MDI and MDI-X automatically. Value range: "On", "Off" Default: "Off"

Administration via WBM

Network > Port configuration



Administration via Local Phone

|--- Admin
|--- Network
|--- Port Configuration
|--- LAN port type
|--- PC port status
|--- PC port type
|--- PC port autoMDIX

3.2.2 VLAN

VLAN (Virtual Local Area Network) is a technology that allows network administrators to partition one physical network into a set of virtual networks (or broadcast domains).

Partitioning a physical network into separate VLANs allows a network administrator to build a more robust network infrastructure. A good example is a separation of the data and voice networks into data and voice VLANs. This isolates the two networks and helps shield the endpoints within the voice network from disturbances in the data network and vice versa.

INFO: The implementation of a voice network based on VLANs requires the network infrastructure (the switch fabric) to support VLANs.

In a layer 1 VLAN, the ports of a VLAN-aware switch are assigned to a VLAN statically. The switch only forwards traffic to a particular port if that port is a member of the VLAN that the traffic is allocated to. Any device connected to a VLAN-assigned port is automatically a member of this VLAN, without being a VLAN aware device itself. If two or more network clients are connected to one port, they cannot be assigned to different VLANs. When a network client is moving from one switch to another, the switches' ports have to be updated accordingly by hand.

With a layer 2 VLAN, the assignment of VLANs to network clients is realized by the MAC addresses of the network devices. In some environments, the mapping of VLANs and MAC addresses can be stored and managed by a central database. Alternatively, the VLAN ID, which defines the VLAN whereof the device is a member, can be assigned directly to the device, e. g. by DHCP. The task of determining the VLAN for which an Ethernet packet is destined is carried out by VLAN tags within each Ethernet frame. As the MAC addresses are (more or less) wired to the devices, mobility does not require any administrator action, as opposed to layer 1 VLAN.

It is important that every switch connected to a PC is VLAN-capable. This is also true for the integrated switch of the OpenScape Desk Phone. The phone must be configured as a VLAN aware endpoint if the phone itself is a member of the voice VLAN, and the PC connected to the phone's PC port is a member of the data VLAN.

There are 3 ways for configuring the VLAN ID of the phone port:

- By LLDP-MED
- By DHCP
- Manually

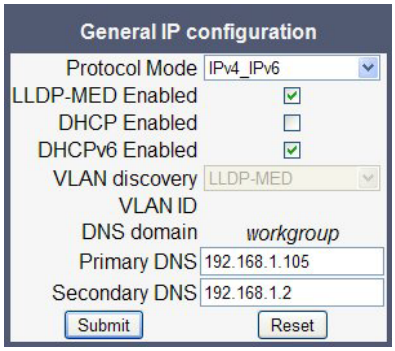
3.2.2.1 Automatic VLAN discovery using LLDP-MED

The VLAN ID can be configured by the network switch using LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery). If this option is selected then the switch has to provide an appropriate TLV (Type-Length-Value) element containing the VLAN ID. If no appropriate TLV is received, DHCP will be used for VLAN discovery.

Administration via WBM

Network > General IP configuration

To enable VLAN discovery via LLDP-MED, activate the **LLDP-MED Enabled**-checkbox and select **LLDP-MED** in the **VLAN discovery** option. Afterwards, click **Submit**.



Administration via Local Phone

To enable VLAN discovery via LLDP-MED, set the **Use LLDP-MED** option to **Yes** and select **LLDP-MED** in the **VLAN discovery** option.

|--- Admin	
|--- Network	
|--- General IP configuration	
|--- Protocol mode	
|--- Use LLDP-MED	
|--- Use DHCP	
|--- Use DHCPv6	
|--- VLAN discovery	
|--- VLAN ID	

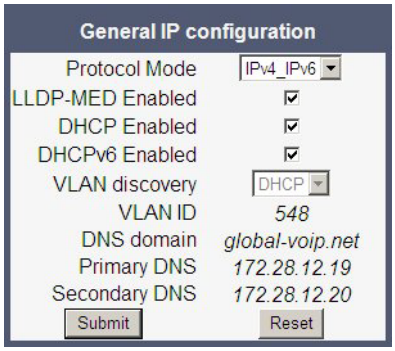
3.2.2.2 Automatic VLAN discovery using DHCP

To automatically discover a VLAN ID using DHCP, the phone must be configured as DHCP enabled, and VLAN discovery mode must be set to "DHCP". LLDP-MED should be disabled. The DHCP server must be configured to supply the Vendor Unique Option in the correct VLAN over DHCP format. If a phone configured for VLAN discovery by DHCP fails to discover its VLAN, it will proceed to configure itself from the DHCP within the non-tagged LAN. Under these circumstances, network routing may probably not be correct.

Administration via WBM

Network > General IP configuration

To enable VLAN discovery via DHCP, activate the **DHCPv6 Enabled** checkbox and select **DHCP** in the **VLAN discovery** option. Afterwards, click **Submit**.



Administration via Local Phone

To enable VLAN discovery via DHCP, activate the **DHCPv6 Enabled** checkbox and select **DHCP** in the **VLAN discovery** option.

└--- Admin	
|--- Network	
|--- General IP configuration	
|--- Protocol mode	
|--- Use LLDP-MED	
|--- Use DHCP	
|--- Use DHCPv6	
|--- VLAN discovery	
|--- VLAN ID	

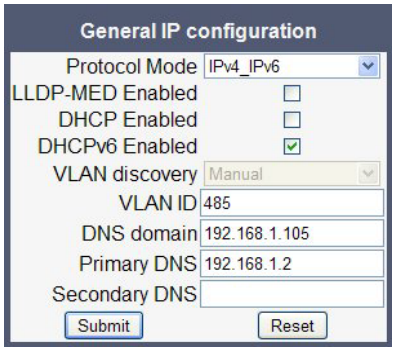
3.2.2.3 Manual Configuration of a VLAN ID

To configure layer 2 VLAN manually, make sure that **VLAN discovery** is set to **Manual** and **LLDP-MED** is **disabled**. Then, the phone must be provided with a VLAN ID between 1 and 4095. If you mis-configure a phone to an incorrect VLAN, the phone will possibly not connect to the network. In DHCP mode it will behave as though the DHCP server cannot be found, in fixed IP mode no server connections will be possible.

Administration via WBM

Network > General IP configuration

The phone must be provided with a VLAN ID between 1 and 4095. Set the **VLAN discovery** to **Manual. Afterwards, click Submit.**



Administration via Local Phone

To enable VLAN discovery via Manual operation, select **Manual** in the **VLAN discovery** option.

|--- Admin	
|--- Network	
|--- General IP configuration	
|--- Protocol mode	
|--- Use LLDP-MED	
|--- Use DHCP	
|--- Use DHCPv6	
|--- VLAN discovery	
|--- VLAN ID	

3.2.3 LLDP-MED Operation

OpenScape Desk Phones support LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for auto-configuration and network management. The auto-configurable parameters are VLAN ID (see *VLAN* and Quality of Service parameters (see *Quality of Service (QoS)*).

The data sent by a network device is stored in neighboring network devices in MIB (Management Information Base) format. In order to keep this information up-to-date, a specific TTL (Time To Live) is specified in LLDP. This value tells a device how long the received information is valid. For OpenScape Desk Phones, the value range is 40, 60, 80, 100, 110, 120, 140, 180, 240, 320, 400.

An example for LLDP-MED operation on OpenScape Desk Phones can be found in *An LLDP-Med Example*.

Administration via WBM

Network > LLDP-MED operation

Administration via Local Phone

|--- Admin	
|--- Network	
|--- LLDP-MED operation	
|--- TTL	
|--- TTL	

3.3 IP Network Parameters

3.3.1 Quality of Service (QoS)

The QoS technology based on layer 2 and the two QoS technologies Diffserv and TOS/IP Precedence based on layer 3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

INFO: Layer 2 and 3 QoS for voice transmission can be set via LLDP-MED (see *LLDP-MED*). If so, the value can not be changed by any other interface.

3.3.1.1 Layer 2 / IEEE 802.1p

QoS on layer 2 is using 3 Bits in the IEEE 802.1q/p 4-Byte VLAN tag which has to be added in the Ethernet header.

The CoS (class of service) value can be set from 0 to 7. 7 is describing the highest priority and is reserved for network management. 5 is used for voice (RTP-streams) by default. 3 is used for signaling by default.

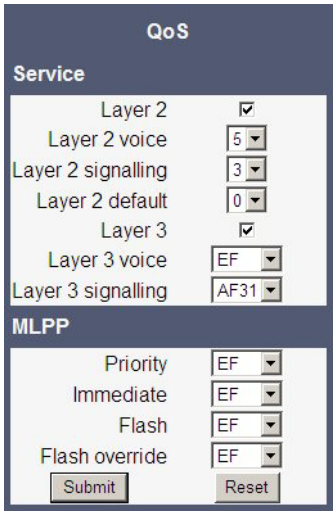
				Three Bits Used for CoS (User Priority)			
PREAM.	SFD	DA	SA	TAG 4 Bytes	PT	DATA	FCS

Data required

- Layer 2: Activates or deactivates QoS on layer 2. Value range: "Yes", "No" Default: "Yes"
- Layer 2 voice: Sets the CoS (Class of Service) value for voice data (RTP streams). Value range: 0-7 Default: 5
- Layer 2 signalling: Sets the CoS (Class of Service) value for signaling. Value range: 0-7 Default: 3
- Layer 2 default: Sets the default CoS (Class of Service) value. Value range: 0-7 Default: 0

Administration via WBM

Network > QoS



Administration via Local Phone

|--- Admin	
|--- Network	
|--- QoS	
|--- Service	
|--- Layer 2	
|--- Layer 2 voice	
|--- Layer 2 signalling	
|--- Layer 2 default	

3.3.1.2 Layer 3 / Diffserv

Diffserv assigns a class of service to an IP packet by adding an entry in the IP header.

Traffic flows are classified into 3 per-hop behavior groups:

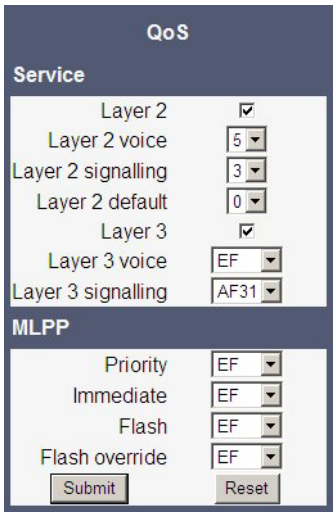
1. Default
   Any traffic that does not meet the requirements of any of the other defined classes is placed in the default per-hop behaviour group. Typically, the forwarding has best-effort forwarding characteristics. The DSCP (Diffserv Codepoint) value for Default is "0 0 0 0 0 0".
2. Expedited Forwarding (EF referred to RFC 3246)
   Expedited Forwarding is used for voice (RTP streams) by default. It effectively creates a special low-latency path in the network. The DSCP (Diffserv Codepoint) value for EF is "1 0 1 1 1 0".
3. Assured Forwarding (AF referred to RFC 2597)
   Assured forwarding is used for signaling messages by default (AF31). It is less stringent than EF in a multiple dropping system. The AF values are containing two digits X and Y (AFXY), where X is describing the priority class and Y the drop level.
   Four classes X are reserved for AFXY: AF1Y (low priority), AF2Y, AF3Y and AF4Y (high priority).
   Three drop levels Y are reserved for AFXY: AFX1 (low drop probability), AFX2 and AFX3 (High drop probability). In the case of low drop level, packets are buffered over an extended period in the case of high drop level, packets are promptly rejected if they cannot be forwarded.

Data required

- Layer 3: Activates or deactivates QoS on layer 3.
  Value range: "Yes", "No"
  Default: "Yes"
- Layer 3 voice: Sets the CoS (Class of Service) value for voice data (RTP streams).
  Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63.
  Default: "EF"
- Layer 3 signalling: Sets the CoS (Class of Service) value for signaling. Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63.
  Default: "AF31"

Administration via WBM

Network > QoS



Administration via Local Phone

|--- Admin	
|--- Network	
|--- QoS	
|--- Service	
|--- Layer 3	
|--- Layer 3 voice	
|--- Layer 3 signalling	

3.3.2 Protocol Mode IPv4/IPv6

An **IPv4 address** consists of 4 number blocks, each between 0 and 255, separated by ".". Example:

Example: 1.222.44.123

An **IPv6 address** consists of 8 hexadecimal number blocks, separated by ":".

Example:

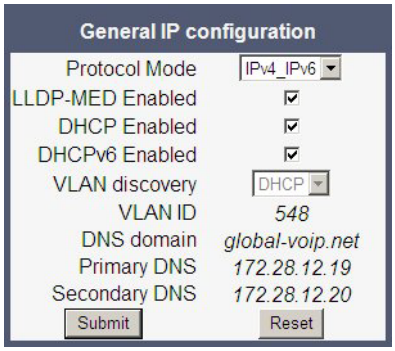
2001:0db8:85a3:08d3:1319:8a2e:0370:7347 or, if not all blocks are used:

2000:1::3

Administration via WBM

Network > General IP configuration

Set the **Protocol Mode** to **IPv4** or **IPv6** or both (the default setting is **IPv4_IPv6**). Afterwards, click **Submit**.



Administration via Local Phone

|--- Admin
|--- Network
|--- General IP Configuration
|--- Protocol Mode

3.3.3 Use DHCP

If this parameter is set to "Yes" (default), the phone will search for a DHCP server on startup and try to obtain IP data and further configuration parameters from that central server.

If no DHCP server is available in the IP network, please deactivate this option. In this case, the IP address, subnet mask and default gateway/route must be defined manually.

> ***INFO:*** The phone is able to maintain its IP connection even in case of DHCP server failure. For further information, please refer to *DHCP Resilience*.

The following parameters can be obtained by DHCP:

Basic Configuration

- IP Address
- Subnet Mask

Optional Configuration

- Default Route (Routers option 3)
- IP Routing/Route 1 & 2 (Static Routes option 33, Classless static route option 121, Private/Classless Static Route (Microsoft) option 249)
- SNTP IP Address (NTP Server option 42)

- Timezone offset (Time Server Offset option 2)
- Primary/Secondary DNS (DNS Server option 6)
- DNS Domain Name (DNS Domain option 15)
- SIP Addresses / SIP Server & Registrar (SIP Server option 120)
- VLAN ID, DLS address (Vendor specific Information option 43)

The following parameters can be obtained by DHCPv6:

Basic Configuration

- Global Address
  Global Address Prefix Length

Optional Configuration

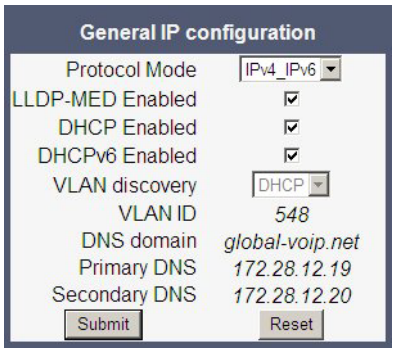
- Primary/Secondary DNS (DNS recursive name server option 23)
- SNTP IP Address (Simple Network Time Protocol Server option 31)
- SIP Addresses / SIP Server & Registrar (SIP Server Domain Name List option 21, SIP Server IPv6 Address List option 22)
- VLAN ID, DLS address (Vendor specific Information option 17)

DHCPv6 options are preferred in Dual Stack Mode if a parameter is configured both via DHCP and via DHCPv6, for instance DNS or SNTP server addresses.

Administration via WBM - IPv4

Network > General IP configuration

Set **DHCP Enabled** to selected. Afterwards, click **Submit**.



Administration via Local Phone - IPv4

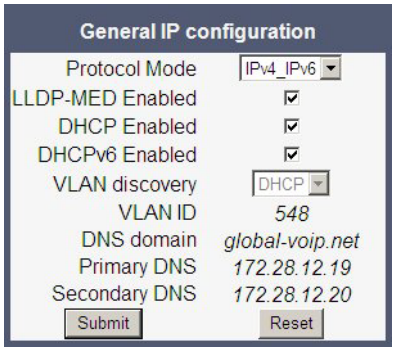
|--- Admin
|--- Network
|--- IPv4 configuration

or/and

Administration via WBM - IPv6

Network > General IP configuration

Set **DHCPv6 Enabled** to selected (the default setting is **Enabled**). Afterwards, click **Submit**.



Administration via Local Phone - IPv6

|--- Admin
|--- Network
|--- IPv6 configuration

3.3.4 IP Address - Manual Configuration

3.3.4.1 How to Manually Configure the Phone´s IP Address

Prerequisites

- If not provided by DHCP dynamically, the phone's IP address and subnet mask must be specified manually.

  INFO: IP addresses can be entered in the following formats:

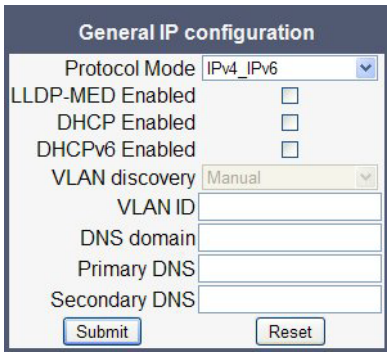
  – Decimal format. Example: 11.22.33.44 or 255.255.255.0 (no leading zeroes).
  – Octal format. Example: 011.022.033.044 (leading zeroes must be used with every address block)
  – Hexadecimal format. Example: 0x11.0x22.0x33.0x44 (prefix 0x must be used with every address block)

- By default, IP configuration by DHCP and LLDP-MED is enabled. For manual IP configuration, please proceed as follows:

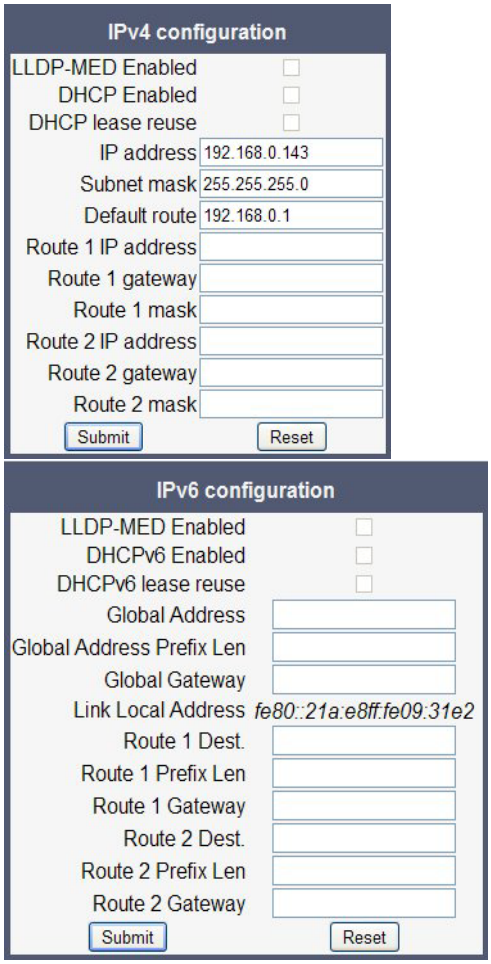
Administration via WBM

Step by Step

1) Navigate to **Network > General IP Configuration**. Set **DHCP Enabled**, **DHCPv6 Enabled** and **LLDP-MED Enabled** to "not selected". Afterwards, click **Submit**.



2) Navigate to Network > IPv4 configuration or IPv6 configuration, depending on the settings in *Protocol Mode IPv4/IPv6*. Set DHCP Enabled , resp. DHCPv6 Enabled and LLDP-MED Enabled to "not selected". Enter the IP address and the Subnet mask. If applicable, enter the Default route. Afterwards, click Submit.



3) After the phone's network service has restarted, the other IP parameters can be configured.

Administration via Local Phone

|--- Admin
|--- Network
General IP configuration
|--- Use LLDP-MED
|--- Use DHCP
|--- Use DHCPv6

└--- Admin
|--- Network
IPv4 configuration
|--- IP address
|--- Subnet mask

└--- Admin
|--- Network
IPv6 configuration
|--- Global address
|--- Global Prefix Len

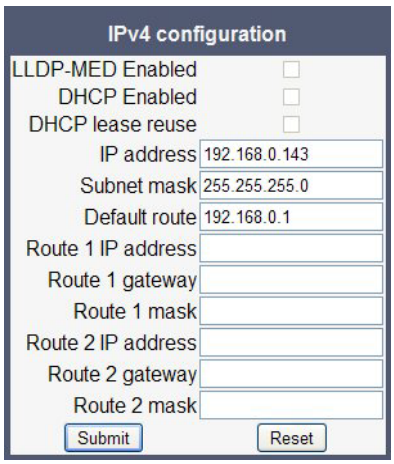
3.3.5 Default Route/Gateway

If not provided by DHCP dynamically (see *Use DHCP*), enter the IP address of the router that links your IP network to other networks. If the value was assigned by DHCP, it can only be read.

Administration via WBM - IPv4 Configuration

Network > IPv4 configuration

Enter the **Default route**, i.e. the IP address of the router that links your IP network to other networks. Afterwards, click **Submit**.



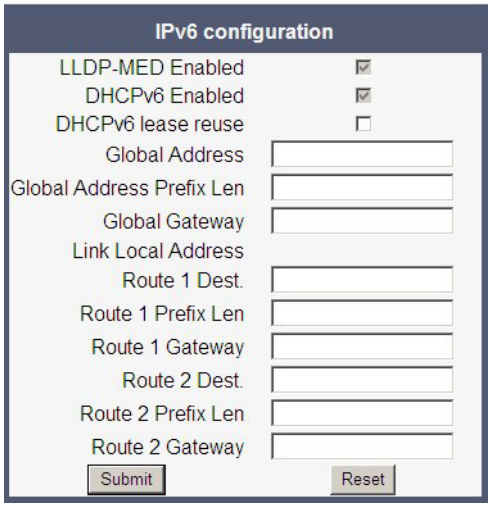
Administration via Local Phone - IPv4 Configuration

|--- Admin
|--- Network
|--- IPv4 configuration
|--- Route (Default)

Administration via WBM - IPv6 Configuration

Network > IPv6 configuration

Enter the IP address of the **Global Gateway** that links your IP network to other networks. Afterwards, click **Submit**.



Administration via Local Phone - IPv6 Configuration

|--- Admin
|--- Network
|--- IPv6 configuration
|--- Global Gateway

3.3.6 Specific IP Routing

To have constant access to network subscribers of other domains, you can enter a total of two more network destinations, in addition to the default route/gateway. This is useful if the LAN has more than one router.

IPv4 Route Configuration

Data required

- **Route 1/2 IP address**: IP address of the selected route.
- **Route 1/2 gateway**: IP address of the gateway for the selected route.
- **Route 1/2 mask**: Network mask for the selected route.

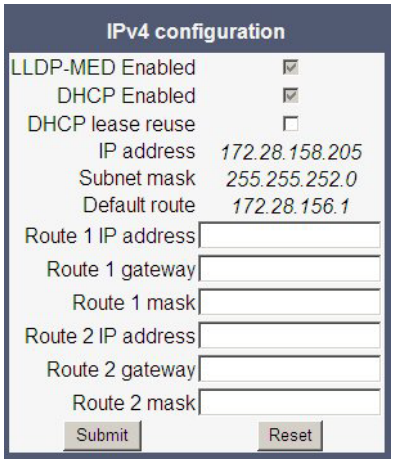
Administration via WBM

Network > IPv4 configuration

Enter the required data:

- For Route 1: **Route 1 IP address**, **Route 1 Gateway**, and **Route 1 mask**.
- For Route 2: **Route 2 IP address**, **Route 2Gateway**, and **Route 2 mask**.

Click **Submit**.



Administration via Local Phone

|--- Admin
|--- Network
|--- IPv4 configuration
|--- Route 1 IP
|--- Route 1 gateway
|--- Route 1 mask
|--- Route 2 IP
|--- Route 2 gateway
|--- Route 2 mask

IPv6 Route Configuration

Data required

- **Route 1/2 destination**: IPv6 address of the selected route.

- **Route 1/2 prefix len**: Prefix length for the selected route.
- **Route 1/2 gateway**: IPv6 address of the gateway for the selected route.

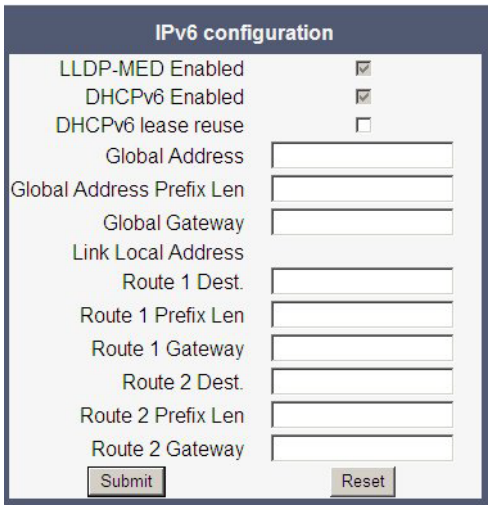
Administration via WBM

Network > IPv6 configuration

Enter the required data:

- For Route 1: **Route 1 Dest.**, **Route 1 Prefix Len**, and **Route 1 Gateway**.
- For Route 2: **Route 2 Dest.**, **Route 2 Prefix Len**, and **Route 2 Gateway**.

Click **Submit**.



Administration via Local Phone

|--- Admin
|--- Network
|--- IPv6 configuration
|--- Route 1 dest
|--- Route 1 prefix len
|--- Route 1 gateway
|--- Route 2 dest
|--- Route 2 prefix len
|--- Route 2 gateway

3.3.7 DNS

The main task of the domain name system (DNS) is to translate domain names to IP addresses. For some features and functions of the OpenScape Desk phone, it is necessary to configure the DNS domain the phone belongs to, as well as the name servers needed for DNS resolving.

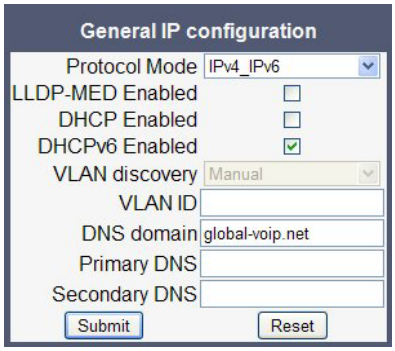
3.3.7.1 DNS Domain Name

This is the name of the phone's local domain.

Administration via WBM

Network > General IP configuration

Enter the **DNS domain** the phone belongs to. Afterwards, click **Submit**.



Administration via Local Phone

|--- Admin
|--- Network
|--- General IP configuration
|--- DNS domain

3.3.7.2 DNS Servers

If not provided by DHCP automatically, a primary and a secondary DNS server can be configured.

> ***INFO:*** Depending on the configuration chosen for survivability, DNS SRV is required. For details, please refer to *Resilience and Survivability*.

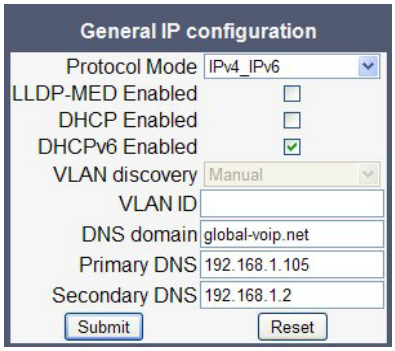
Data required

- Primary DNS: IP address of the primary DNS server.
- Secondary DNS: IP address of the secondary DNS server.

Administration via WBM

Network > General IP configuration

Enter the **Primary DNS** and **Secondary DNS** IP addresses for the primary and the secondary DNS server. Afterwards, click **Submit**.



Administration via Local Phone

|--- Admin
|--- Network
|--- General IP configuration
|--- Primary DNS
|--- Secondary DNS

3.3.7.3 Terminal Hostname

> ***INFO:*** DHCP and DNS must be appropriately connected and configured at the customer site.

The phone's hostname can be customised.

The corresponding DNS domain is configured in Network > General IP configuration > DNS domain (see *3.3.7.1 DNS Domain Name*).

The current DNS name of the phone is displayed at the right-hand side of the banner of the admin and user web pages, under **DNS name**. To see configuration changes, the web page must be reloaded.

> ***INFO:*** It is recommended to inform the user about the DNS name of his/her phone. If the corresponding infrastructure is available at the customer site, the complete WBM address can be found under **User menu > Network information > Web address**

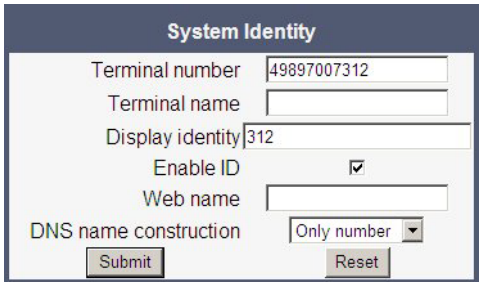
The DNS name can be constructed from pre-defined parameters and free text. Its composition is defined by the **DNS name construction** parameter under the WBM path **Administration > System > System Identity > DNS name construction**. The following options are available:

- **None**.

- **MAC based**: The DNS name is built from the prefix "OIP" followed by the phone's MAC address.
- **Web name**: The DNS name is set to the string entered in **Web name**.
- Only number: The DNS name is set to the Terminal number, that is, the phone's call number (see *Terminal and User Identity*).
- **Prefix number**: The DNS name is constructed from the string entered in **Web name**, followed by the Terminal number.

Administration via WBM

System > System Identity



Administration via Local Phone

|--- Admin	
|--- System	
|--- Identity	
|--- Web name	
|--- DDNS hostname	

3.3.8 Configuration & Update Service (DLS)

The Deployment Service (DLS) is an OpenScape Management application for administering workpoints in communication networks. Amongst the most important features are: security (e.g. PSS generation and distribution within an SRTP security domain), mobility for OpenScape SIP phones, software deployment, plug&play support, as well as error and activity logging.

DLS address, i.e. the IP address or host name of the DLS server, and **DLS port**, i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS.

The **Contact gap** parameter is not used.

The **Security mode** determines the security level for the communication between the phone and the DLS. Mutual authentication establishes a higher security level of the connection by mutually exchanging credentials between the DLS and the

phone. After this, the communication is encrypted, and a different port is used, thus ensuring that the phone is unambiguously connected to the correct DLS server.

INFO: It is possible to operate the DLS server behind a firewall or NAT (Network Address Translation), which prevents the DLS from sending Contact-Me messages directly to the phone. Only outbound connections from the phone are allowed. To overcome this restriction, a DLS Contact-Me proxy (DCMP) can be deployed. The phone periodically polls the DCMP (DLS Contact-Me Proxy), which is placed outside of the phone's network, for pending contact requests from the DLS. If there are contact requests, the phone will send a request to the DLS in order to obtain the update, just as with a regular DLS connection.

INFO: The URI of the DCMP, as well as the polling interval, are configured by the DLS. For this purpose, it is necessary that the phone establishes a first contact to the DLS, e. g. by phone restart or local configuration change.

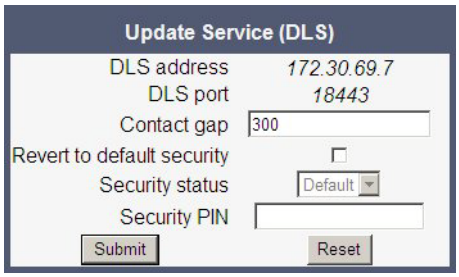
A Security PIN can be provided which is used for decrypting data provided by the DLS during bootstrap. For further information, please refer to the *DLS documentation*.

Data required

- **DLS address**: IP address or host name of the server on which the Deployment Service is running.
- **DLS port**: Port on which the DLS Deployment Service is listening. Default: 18443
- **Contact gap**: The parameter is not used.
- **Security status**: Shows whether the communication between the phone and the DLS is secure. Value range: "Default", "Secure", "Secure PIN" This parameter is read-only.
- **Security PIN**: Used for enhanced security.

Administration via WBM

Network > Update Service (DLS)



Administration via Local Phone

|--- Admin	
|--- Network	
|--- Update Service (DLS)	
|--- DLS address	
|--- DLS port	
|--- Contact gap	
|--- Security status	
|--- Security PIN	

3.3.9 SNMP

The Simple Network Management Protocol is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention. An SNMP manager surveys and, if needed, configures several SNMP elements, e.g. VoIP phones.

OpenScape Desk Phones support SNMPv1.

There are currently 4 trap categories that can be sent by the phones:

Standard SNMP Traps

OpenScape Desk Phones support the following types of standard SNMP traps, as defined in RFC 1157:

- **coldStart**: sent if the phone does a full restart.
- **warmStart**: sent if only the phone software is restarted.
- **linkUp**: sent when IP connectivity is restored.

QoS Related Traps

These traps are designed specifically for receipt and interpretation by the Customer Data Collection system (OpenScape Customer Data Collection (CDC) or HiPath QoS Data Collection). The traps are common to SIP phones, HFA phones, Gateways, etc.

Traps for important high level SIP related problems

Currently, these traps are related to problems in registering with a SIP Server and to a failure in remotely logging off a mobile user. These traps are aimed at a non-expert user (e.g. a standard Network Management System) to highlight important telephony related problems.

Traps specific to OpenScape Desk Phones

Currently, the following traps are defined:

TraceEventFatal: sent if severe trace events occur; aimed at expert users.

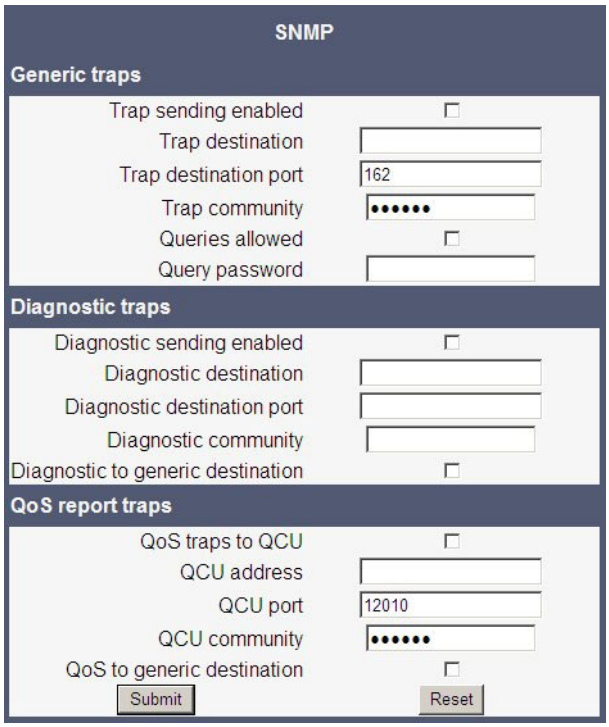
TraceEventError: sent if severe trace events occur; aimed at expert users.

Data required

- **Trap sending enabled**: Enables or disables the sending of a TRAP message to the SNMP manager.
  Value range: "Yes", "No"
  Default: "No"
- **Trap destination**: IP address or host name of the SNMP manager that receives traps.
- **Trap destination port**: Port on which the SNMP manager is receiving TRAP messages.
  Default: 162
- **Trap community**: SNMP community string for the SNMP manager receiving TRAP messages.
  Default: "snmp"
- **Queries allowed**: Allows or disallows queries by the SNMP manager.
- **Query password**: Password for the execution of a query by the SNMP manager.
- **Diagnostic sending enabled**: Enables or disables the sending of diagnostic data to the SNMP manager.
  Value range: "Yes", "No"
  Default: "No"
- **Diagnostic destination**: IP address or host name of the SNMP manager receiving diagnostic data.
- **Diagnostic destination port**: Port on which the SNMP manager is receiving diagnostic data.
- **Diagnostic community**: SNMP community string for the SNMP manager receiving diagnostic data.
- **Diagnostic to generic destination / Diagnostic to generic device**: Enables or disables the sending of diagnostic data to a generic destination.
  Value range: "Yes", "No"
  Default: "No"
- **QoS traps to QCU**: Enables or disables the sending of TRAP messages to the QCU server.
  Value range: "Yes", "No"
  Default: "No"
- **QCU address**: IP address or hostname of the QCU server.
- **QCU port**: Port on which the QCU server is listening for messages.
  Default: 12010.
- **QCU community**: QCU community string.
  Default: "QOSCD".
- **QoS to generic destination**: Enables or disables the sending of QoS traps to a generic destination.
  Value range: "Yes", "No"
  Default: "No"

Administration via WBM

System > SNMP



Administration via Local Phone

└--- Admin	
|--- System	
|--- SNMP	
|--- Queries allowed	
|--- Query password	
|--- Trap sending enabled	
|--- Trap destination	
|--- Trap destination port	
|--- Trap community	
|--- Diag sending enabled	
|--- Diag destination	
|--- Diag destination port	
|--- Diag community	
|--- QoS traps to QCU	
|--- QCU address	

|--- QCU port	
|--- QCU community	
|--- QoS to generic dest.	

3.4 Security

3.4.1 Speech Encryption

3.4.1.1 Security - General Configuration

OpenScape Desk Phones support secure (i.e. encrypted) speech transmission via SRTP. For enabling secure (encrypted) calls, a TLS connection to the OpenScape Voice server is required.

If **Use secure calls** is activated, the encryption of outgoing calls is enabled, and the phone is capable of receiving encrypted calls. When the phone is connected to an OpenScape Voice system, call security is communicated to the user as follows:

- An icon in the call view tells the user whether a call is secure (encrypted) or not.
- If an active call changes from secure to insecure, e. g. after a transfer, a popup window and an alert tone will notify the user.

INFO: For secure (encrypted) calls, it is required that both endpoints support SRTP. The secure call indication tells the user that the other endpoint has acknowledged the secure connection.

INFO: In order to use SRTP, the phone must be configured for NTP (for further information please see *Date and Time*). The reason is that the key generation (MIKEY) uses the system time of the particular device as a basis. Thus, encryption will only work correctly if all devices have the same UTC time.

If **SIP server certificate validation** resp. **Backup SIP server certificate validation** is activated, the phone will validate the server certificate sent by the OpenScape Voice server in order to establish a TLS connection. The server certificate is validated against the root certificate from the trusted certificate authority (CA), which must be stored on the phone first. For delivering the root certificate, a DLS (OpenScape Deployment Service) server is required.

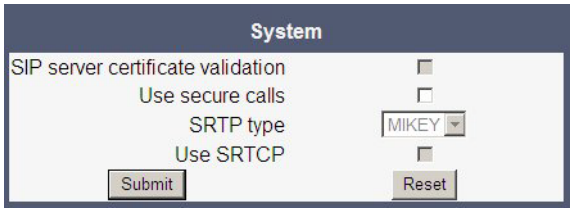
The **SRTP type** sets the key exchange method for SRTP.

When **Use SRTCP** is activated (together with Use secure calls), the phone will use SRTCP (Secure RTCP) to transmit and receive RTP control packets.

> ***INFO:*** If SRTP is enabled, ANAT interworking (see *Media/SDP*) is only possible if SDES is configured as the key exchange protocol for SRTP.

Administration via WBM

System > Security > System



Administration via Local Phone

|--- Admin	
|--- System	
|--- Security	
|--- Server cerfificate	
|--- Use secure calls	
|--- SRTP type	
|--- Use SRTCP	

3.4.1.2 MIKEY Configuration

MIKEY (Multimedia Internet KEYing) is a key management protocol that is intended for use with real-time applications. It can specifically be used to set up encryption keys for multimedia sessions that are secured using SRTP.

Use secure calls activates the encryption of outgoing calls, i.e. the phone is capable of receiving encrypted calls.

> ***INFO:*** For secure (encrypted) calls, it is required that both endpoints support SRTP. The secure call indication tells the user that the other endpoint has acknowledged the secure connection.

The **SRTP type** sets the key exchange method (negotiation method) for secure calls via SRTP. The following encryption key exchange methods are available:

- **MIKEY**
- SDES (see *SDES Configuration*)

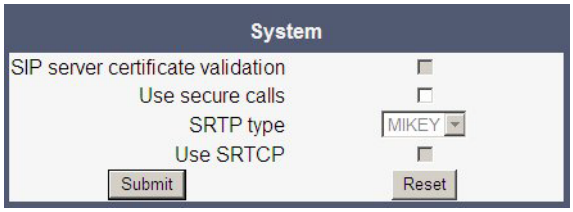
The **SRTP Type** and **Use SRTCP** options are only available for secure (encrypted) calls, i.e. these parameters are only enabled if **Use secure calls** is activated.

When **Use SRTCP** is activated (together with **Use secure calls**), the phone will use SRTCP (Secure RTCP) to transmit and receive RTP control packets.

> ***INFO:*** If SRTP is enabled, ANAT interworking (see *Media/SDP*) is only possible if SDES is configured as the key exchange protocol for SRTP.

Administration via WBM

System > Security > System



Administration via Local Phone

|--- Admin	
|--- System	
|--- Security	
|--- Server cerfificate	
|--- Use secure calls	
|--- SRTP type	
|--- Use SRTCP	

3.4.1.3 SDES Configuration

When SDES is selected as SRTP negotiation method (see *Security - General Configuration*), it can be configured further.

The SDES status parameter enables or disables SDES, just like SRTP type in System > Security > System (see *Security - General Configuration*). When SDES is disabled, MIKEY will be used.

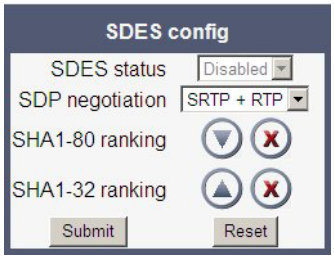
The SDP negotiation parameter specifies whether the use of SRTP will be forced by the phone. The following choices are available:

- **RTP + SRTP** - Both non-encrypted (non-secure) and encrypted (secure) media connections are offered. Non-encrypted connections are preferred over encrypted connections, i.e. the phone uses the non-encrypted RTP connection if the remote party accepts it and only switches to SRTP if RTP is not accepted.
- With **SRTP only**, only an encrypted (secure) media connection is allowed; if the remote party should not support SRTP, no connection will be established.
- With **SRTP + RTP**, the phone will try to establish an SRTP connection, but fall back to RTP if this should fail. This is the recommended option.

With **SHA1-80 ranking** and **SHA1-32 ranking**, the ranking for each crypto-suite for negotiation is defined. Additionally, each crypto-suite can be enabled or disabled.

Administration via WBM

System > Security > SDES config



3.4.2 Access Control

The **CCE access** parameter controls TCP and UDP access for the CCE (CommsChannel Extender). This affects the operation of the OpenStage Manager, local CTI access, and HPT access. When **Disable** is selected, both TCP and UDP are disabled. With **Enable**, there are no restrictions.

With **Factory reset claw**, the 'hooded claw' keypad mechanism to initiate a factory reset without requiring an authenticated access can be enabled or disabled.

The **Serial port** parameter controls access to the serial port. When set to **No password**, a terminal connected to the port can interact with the phone's operating system without restrictions. When **Passwd reqd** is selected, the serial port requires a password for access (root user is not available). When **Unavailable** is chosen, the serial port is not accessible.

As a prerequisite, the root user needs to create a user and to define a password via Serial Access, so that access can be granted when the **Password required** prompt is issued.

Administration via WBM

System > Security > Access control

3.4.3 Security Log

A circular security log is used to capture important security specific events. It can be exported as CSV data to an external application for analysis.

INFO: The security log cannot be disabled.

The **Max. lines** parameter defines the maximum number of entry lines that can be kept in the security log before old entries are overwritten by new entries.

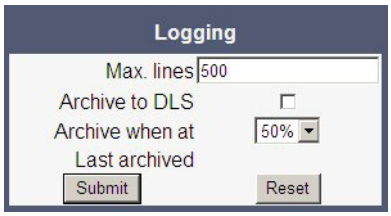
Archive to DLS controls whether the log is sent to the DLS. When activated, the DLS is used to automatically archive the security log so that no log entries will be lost.

With **Archive when at**, the trigger for log archiving is set. Automatic archiving of new security log entries will occur when the percentage of unarchived entries in the log is as specified or more. When set to 0%, every new entry will trigger a save. The possible values are ”0%", "10%”, ”20%”, ”30%”, ”35%”, ”40%”, ”45%”, ”50%”, ”55%”, ”60%”, ”65%”, ”70%”, ”80%”, ”90%”.

Last archived shows the date when the security log was last archived to the DLS.

Administration via WBM

System > Security > Logging



3.4.4 Security-Related Faults

INFO: The entries in this list are only displayed until they are reported to the DLS, which usually happens very fast. After that, the entries are automatically deleted from the phone. If the entries are not deleted automatically, they can be deleted manually by using the **Cancel faults** parameter.

Security log entry shows the date and time of a loss of security log entries.

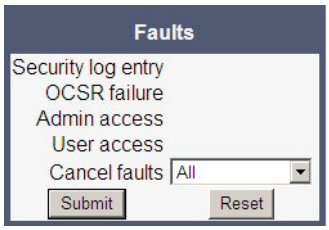
OCSR failure shows the date and time when the phone was unable to connect to any certificate checking server for revoked certificates.

Admin access shows the date and time when the phone encountered multiple consecutive failures to enter the admin password.

User access shows the date and time when the phone encountered multiple consecutive failures to enter the user password.

Administration via WBM

System > Security > Faults



3.4.5 Password Policy

3.4.5.1 General Policy

Expires after (days) sets the maximum validity period of a password.

Warn before (days) specifies when the user/admin is notified that his password will expire.

Force changed only affects the User password. When Force changed is activated, the user will be forced to change his/her password at next login.

Tries allowed specifies the maximum number of password entry trials before the password is suspended. Values: 0 (no limits), 2, 3, 4, 5

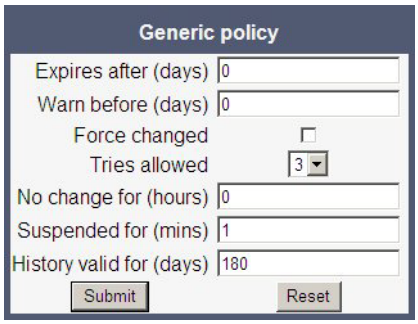
No change for (hours) specifies a period before a password is allowed to be changed again. Value range: 0 to 99

Suspended for (mins) defines how long a password will be suspended after the number of failed retries has exceeded. Value range: 0 to 99

History valid for (days) defines a period in days during which the history is valid. Passwords no longer used are kept in history lists for the user and admin passwords to prevent reuse of past passwords. This list is organised as FIFO (First In, First Out) so that it always contains the latest passwords.

Administration via WBM

Security and Policies > Password > Generic Policy



3.4.5.2 Admin Policy

Expiry date shows the date and time when the admin password will expire.

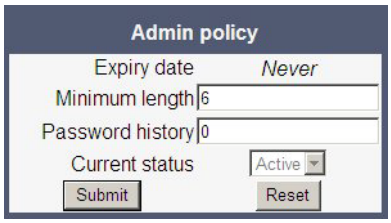
Minimum length defines the minimum number of characters for the admin password.

Password history specifies the number of entries to be kept in the admin password history. New passwords must not match any password in the history.

The **Current status** parameter determines the status for the admin password. When set to **Active**, the admin password is available for use. With **Suspended**, the admin password is not available for a period or until reset. When set to **Disabled**, all access via the admin password is disabled. The status of the admin password can only be set via DLS/WPI. It is changed internally to **Suspended** when the password has been entered incorrectly more times than allowed.

Administration via WBM

Security and Policies > Password > Admin Policy



3.4.5.3 User Policy

Expiry date shows the date and time when the user password will expire.

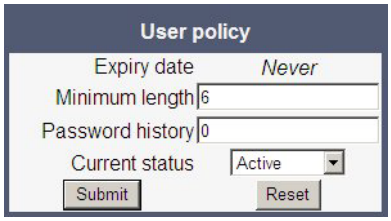
Minimum length defines the minimum number of characters for the user password.

Password history specifies the number of entries to be kept in the user password history.

The **Current status** parameter determines the status for the user password. When set to **Active**, the user password is available for use. With **Suspended**, the user password is not available for a period or until reset. When set to **Disabled**, all access via the user password is disabled.

Administration via WBM

Security and Policies > Password > User Policy



3.4.5.4 Character Set

The composition of the password can be configured in detail.

Ucase chars reqd. defines the minimum number of uppercase characters. Value range: 0 to 24

Lcase chars reqd. defines the minimum number of lowercase characters. Value range: 0 to 24

Digits required defines the minimum number of digits. Value range: 0 to 24

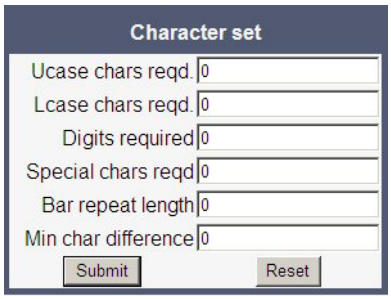
Special chars reqd defines the minimum number of special characters. The set of possible characters is ` - = [ ] ; ’ # \ , . / ¬ ! ” £ $ % ^ & * ( ) _ + { } : @ ~ | < > ? Value range: 0 to 24

Bar repeat length specifies the maximum number of consecutive uses of a character. Value range: 0 to 24, but not 1 (with 1 set as value, no password would be valid, because it would be forbidden to use any character once).

Min char difference specifies the minimum number of characters by which a new password must differ from the previous password. Value range: 0 to 24

Administration via WBM

Security and Policies > Password > Character set

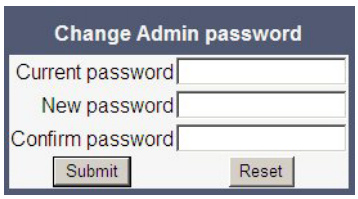


3.4.5.5 Change Admin and User password

The passwords for user and administrator can be set here. They have to be confirmed after entering. The factory setting for the Admin password is "123456"; it should be changed after the first login (Password handling in previous versions see *Password*).

Administration via WBM

Security and Policies > Password > Change Admin password



Security and Policies > Password > Change User password

Administration via Local Phone

|--- Admin	
|--- Security & policies	
|--- Password	
|--- Change Admin password	
| |--- Current password	
| |--- New password	
| |--- Confirm password	
|--- Change User password	

|--- Admin password	
|--- New password	
| |--- Confirm password	

3.4.6 Certificate Policy

3.4.6.1 Online Certificate Check

The Online Certificate Status Protocol (OCSP) is used to check if a certificate to be used has been revoked. This protocol is used to query an Online Certificate Status Responder (OCSR) at the point when the certificate is being validated. The address of an OCSR can be configured on the phone and can also be obtained from the certificate to be checked (which will have the priority).

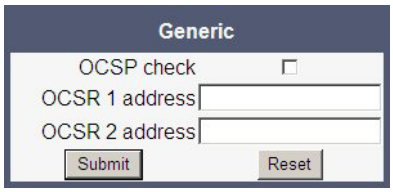
When **OCSP check** is activated, the configured OCSR is requested to check if the certificate has been revoked.

OCSR 1 address specifies the IP address (or FQDN) of a primary OCSP responder.

OCSR 2 address specifies the IP address (or FQDN) of a secondary OCSP responder.

Administration via WBM

Security and Policies > Certificates > Generic



3.4.6.2 Server Authentication Policy

For individual certificates provided by specific servers, the level of authentication can be configured. When **None** is selected, no certificate check is performed. With **Trusted**, the certificate is only checked against the signature credentials provided by the remote entity for signature, and the expiry date is checked. When **Full** is selected, the certificate is fully checked against the credentials provided by the remote entity for signature, the fields must match the requested subject/ usage, and the expiry date is checked.

Secure file transfer sets the authentication level for the HTTPS server to be used (see *Common FTP/HTTPS Settings*).

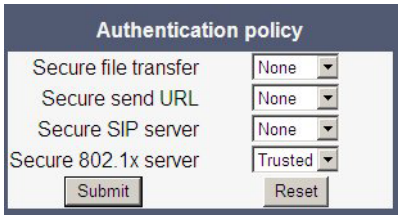
Secure send URL sets the authentication level for the server to which special HTTP requests are sent on key press ("Send URL" function, see *Send URL Request via HTTP/HTTPS*).

Secure SIP server sets the authentication level for the SIP server connected to the phone (see *SIP Registration*).

Secure 802.1x server sets the authentication level for the 802.1x authentication server.

Administration via WBM

Security and Policies > Certificates > Authentication policy



Administration via Local Phone

|--- Admin
|--- Security & policies
|--- Certificates
|--- Authentication policy
|--- Secure file transfer
|--- Secure send URL

3.5 System Settings

3.5.1 Terminal and User Identity

3.5.1.1 Terminal Identity

Within a SIP environment, both Terminal Number and Terminal Name may serve as a phone number. The values are used in the userinfo part of SIP URIs.

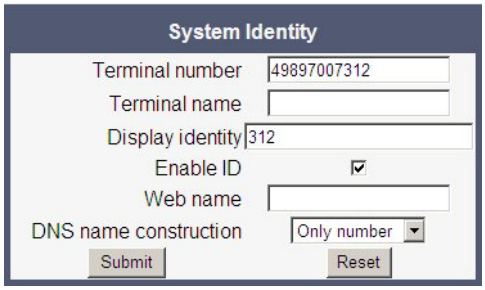
In order to register with a SIP registrar, the phone sends REGISTER messages to the registrar containing the contents of Terminal number.

Data required

- Terminal number: Number to be registered at the SIP registrar.
- Terminal name: Name to be registered at the SIP registrar.

Administration via WBM

System > System Identity



Administration via Local Phone

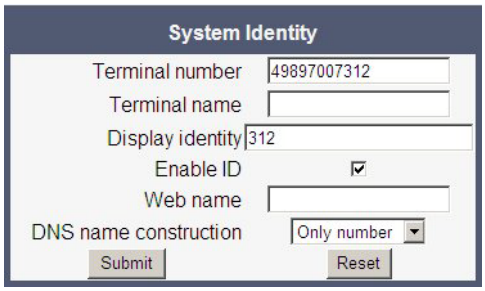
|--- Admin	
|--- System	
|--- Identity	
|--- Terminal number	
|--- Terminal name	

3.5.1.2 Display Identity

If an individual name or number is entered as **Display identity** and **Enable ID** is activated, it is displayed in the phone's status bar instead of the Terminal number.

Administration via WBM

System > System Identity



Administration via Local Phone

|--- Admin	
|--- System	
|--- Identity	
|--- Display identity	
|--- Enable ID	

3.5.2 Emergency and Voice Mail

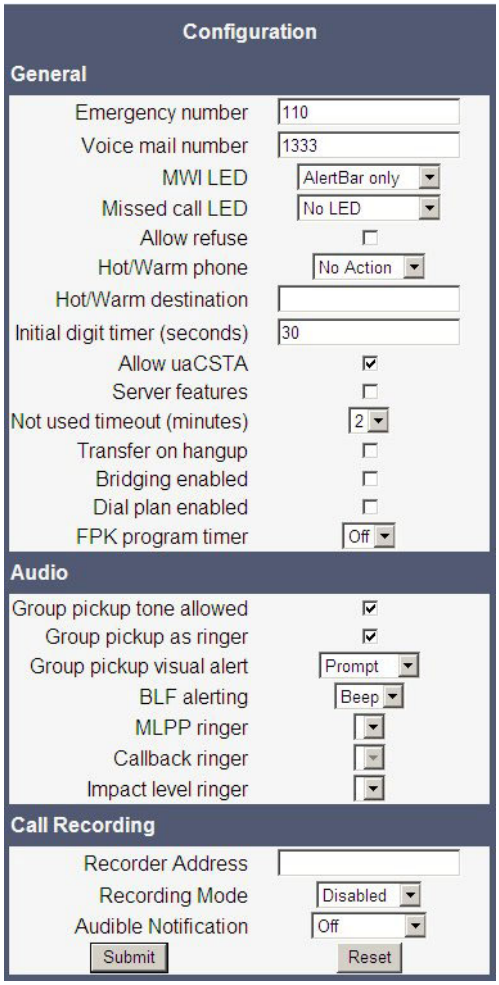
It is important to have an **Emergency number** configured. If the phone is locked, a clickable area for making an emergency call is created.

> ***INFO:*** If more than one emergency number is needed, additional numbers can be configured in the canonical dial settings (*Canonical Dialing Configuration*).

If a mailbox located at a remote server shall be used, its **Voice mail number** must be entered.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Emergency number	
|--- Voicemail number	

3.5.3 Call logging

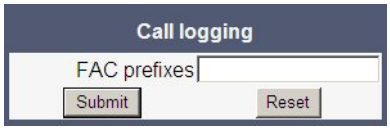
This configuration item allows the phone to detect if a number dialed by the user is likely to be a Feature Access Code (FAC) by comparing the start of the dialed number with the configured FAC prefixes. If the dialed number does match a FAC prefix and the SIP server has provided a different number for the called party then the number shown in the Dialled tab list of Call Log is changed from the dialed number to the server-provided number. If the new configuration item is left empty then the Dialled tab list display will remain as currently populated (i.e. the dialed number is shown in the list).

A further enhancement for an entry matched to a FAC in the Dialled tab list of Call Log is that the context menu for the list entry now provides both numbers from the last call associated with the entry as Dial options in the context menu for the list entry (similar to that already provided by the context menu for the Details form of such an entry). Note that the Call Log display on the OpenScape Desk Phone IP 35G has been simplified so that an entry only displays a name or a number (not both) and there is no access to entry details. However this only limits the display and the default dialing number for an OpenScape Desk Phone IP 35G entry is determined as above.

Call Log entry grouping rules for the Dialled tab list remain unchanged, if multiple FACs all map to numbers associated with one contact then they are grouped together.

Administration via WBM

Local functions > Call logging



3.5.3.1 Logging of Missed Calls Answered Elsewhere (via User menu)

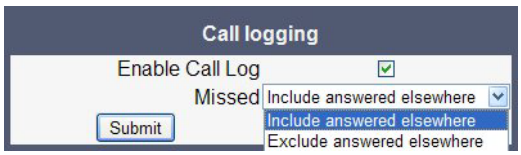
This feature allows the user to

- distinguish logged calls based on the device on which the calls were completed, and
- decide whether missed calls that were answered elsewhere shall be
  - included in the call log, OR
  - excluded from the call log, i.e. not logged at all.

In the **Call Lists**, missed calls that were completed elsewhere are marked with a check mark. For details, please refer to the *User manual*.

Administration via WBM (User menu)

User > Configuration > Call logging



Administration via Local Phone (User menu)

|--- User	
|--- Configuration	
|--- Missed	
|--- Include answered elsewhere	
|--- Exclude answered elsewhere	

Include answered elsewhere: Calls completed elsewhere will be logged as missed calls. In the call log these calls are marked with a check mark.

Exclude answered elsewhere: Calls completed elsewhere will not be visible on phone; they will not be logged at all.

3.5.4 Date and Time

If the DHCP server in your network provides the IP address of the SNTP server, no manual configuration is necessary. If not, you have to set the **SNTP IP address** parameter manually.

For correct display of the current time, the **Timezone offset** must be set appropriately. This is the time difference between the local time and UTC (Universal Time Coordinated). If, for instance, the phone is located in Munich, Germany, the offset is +1 (or simply 1); if it is located in Los Angeles, USA, the offset is -8. For countries or areas with half-our time zones, like South Australia or India, non-integer values can be used, for example 10.5 for South Australia (UTC +10:30).

If the phone is located in a country with DST (Daylight Saving Time), you can choose whether DST is toggled manually or automatically. For manual toggling, disable **Auto time change** and enable or disable **Daylight saving**; the change will be in effect immediately. For automatic toggling, enable **Auto time change**;

now, daylight saving is controlled by the DST zone / Time zone parameter. This parameter determines when DST starts or ends, and must be set according to the location of the phone.

The **Difference (minutes)** parameter defines how many minutes the clock is put forward for DST. In Germany, for instance, the value is +60.

INFO: Please note that **Difference (minutes)** must be specified both for manual and automatic DST toggling.

3.5.4.1 SNTP is Available, but No Automatic Configuration by DHCP Server

Data required

- **SNTP IP address**: IP address or hostname of the SNTP server.
- **Timezone offset (hours)**: Shift in hours corresponding to UTC.
- **Daylight saving**: Enables or disables daylight saving time in conjunction with **Auto time change**. Value range: "Yes", "No"
  Default setting is **Yes**. After a factory reset, the system will be reset to this value.
- **Difference (minutes)**: Time difference when daylight saving time is in effect.
  Default setting is **60 (mins)**. After a factory reset, the system will be reset to this value.
- **Auto time change / Auto DST**: Enables or disables automatic control of daylight saving time according to the Time zone. Value range: "Yes", "No"
  Default setting is **Yes**. After a factory reset, the system will be reset to this value.
- **Time zone / DST zone**: Area with common start and end date for daylight saving time. Value range: "Australia 2007 (ACT, South Australia, Tasmania, Victoria)", "Australia 2007 (New South Wales)", "Australia (Western Australia)", "Australia 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)", "Brazil", "Canada", "Canada (Newfoundland)", "Europe (Portugal, United Kingdom)", "Europe (Finland)", "Europe (Rest)", "Mexico", "United States", "New Zealand", "New Zealand (Chatham)".
  Default setting for **US** is **United States**. After a factory reset, the system will be reset to this value.

Administration via WBM

Date and Time

Administration via Local Phone

|--- Admin	
|--- Date and Time	
|--- SNTP IP address	
|--- Timezone offset	

3.5.4.2 No SNTP Server Available

If no SNTP server is available, date and time must be set manually.

INFO: The parameters for the manual setting of time and date are located in the User menu, not in the Administrator menu.

Data required

- Local time (hh:mm): Local time.
- Local date (day, month, year): Local date.
- Allow daylight saving: Defines whether there is daylight is set.
- Difference (minutes): Timezone offset in minutes.

Administration via WBM

(User pages >) Date and time

Administration via Local Phone

└--- User	
|--- Date and Time	
|--- Time	
|--- Date	
|--- Daylight saving	
|--- Difference (mins)	

3.5.5 SIP Addresses and Ports

3.5.5.1 SIP Addresses

In this group of parameters, the IP addresses or host names for the SIP server, the SIP registrar, and the SIP gateway are defined.

SIP server address provides the IP address or host name of the SIP proxy server (OpenScape Voice). This is necessary for outgoing calls. **SIP registrar address** contains the IP address or host name of the registration server, to which the phone will send REGISTER messages. When registered, the phone is ready to receive incoming calls. **SIP gateway address** gives the IP address or host name of the SIP gateway. If configured, the SIP gateway is used for outgoing calls; otherwise the server specified in **SIP server address** is used. A SIP gateway is able to perform a conversion of SIP to TDM, which enables to send calls directly into the public network.

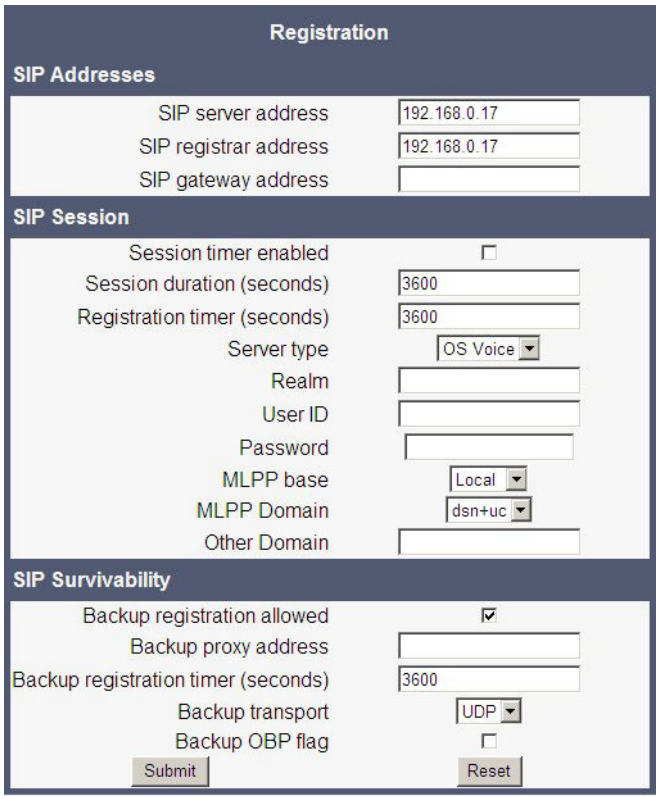
INFO: Enhanced survivability using DNS SRV is available. To make use of it, a special configuration is required. For details, please refer to *Resilience and Survivability*.

Data required

- **SIP server address**: IP address or host name of the SIP proxy server.
- **SIP registrar address**: IP address or host name of the registration server.
- **SIP gateway address**: IP address or host name of the SIP gateway.

Administration via WBM

System > Registration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Registration	
|--- SIP Addresses	
|--- SIP server	
|--- SIP registrar	
|--- SIP gateway	

3.5.5.2 SIP Ports

In this group of parameters, the ports for the SIP server, the SIP registrar, and the SIP gateway are defined (for further information see *SIP Addresses*), as well as the SIP port used by the phone (SIP local).

Data required

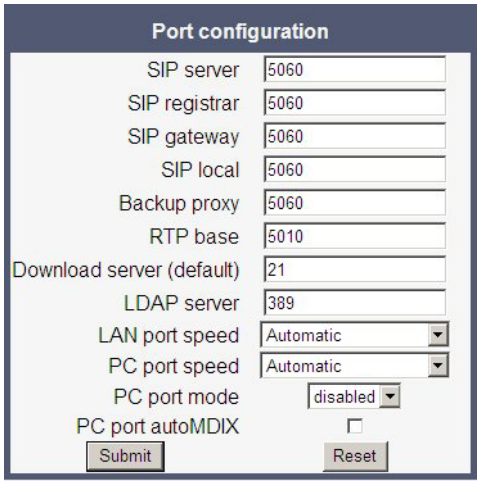
- **SIP server**: Port of the SIP proxy server. Default: 5060.

- **SIP registrar**: Port of the server at which the phone registers. Default: 5060.
- **SIP gateway**: Port of the SIP gateway. Default: 5060.
- **SIP local**: Port used by the phone for sending and receiving SIP messages. Default: 5060.

> ***INFO:*** When changing the SIP Transport protocol from UDP/TCP to TLS, the SIP ports now also have to be changed correspondingly (e.g. SIP port from 5060 to 5061) and on changing vice versa.

Administration via WBM

Network > Port configuration



Administration via Local Phone

|--- Admin	
|--- Network	
|--- Port Configuration	
|--- SIP server	
|--- SIP registrar	
|--- SIP gateway	
|--- SIP local	

3.5.6 SIP Registration

Registration is the process by which centralized SIP Server/Registrars become aware of the existence and readiness of an endpoint to make and receive calls. The phone supports a number of configuration parameters to allow this to happen. Registration can be authenticated or un-authenticated depending on how the server and phone is configured.

For operation with an OpenScape Voice server, set **Server type** to "OS Voice". When HiQ8000 is to be used, set it to "HiQ8000". The expiry time of a registration can be specified by **Registration timer**.

Unauthenticated Registration

For unauthenticated registration, the following parameters must be set on the phone: Terminal number or Terminal name (see *Terminal Identity*), SIP server and SIP registrar address (see *SIP Addresses*).

In unauthenticated mode, the server must pre-authenticate the user. This procedure is server specific and is not described here.

Authenticated Registration

The phone supports the digest authentication scheme and requires some parameters to be configured in addition to those for unauthenticated registration. By providing a **User ID** and a **Password** which match with a corresponding account on the SIP registrar, the phone authenticates itself. Optionally, a **Realm** can be added. This parameter specifies the protection domain wherein the SIP authentication is meaningful. The protection domain is globally unique, so that each protection domain has its own arbitrary user names and passwords.

INFO: A challenge from the server for authentication information is not only restricted to the REGISTER message, but can also occur in response to other SIP messages, e. g. INVITE.

INFO: If registration has not succeeded at startup or registration fails after having been previously successfully registered the phone will try to re-register every 30 seconds. This is not configurable.

If the registration is not answered at all, the phone will try to re-register every 60 seconds by default. This is configurable (see *Maximum Registration Backoff Timer*).

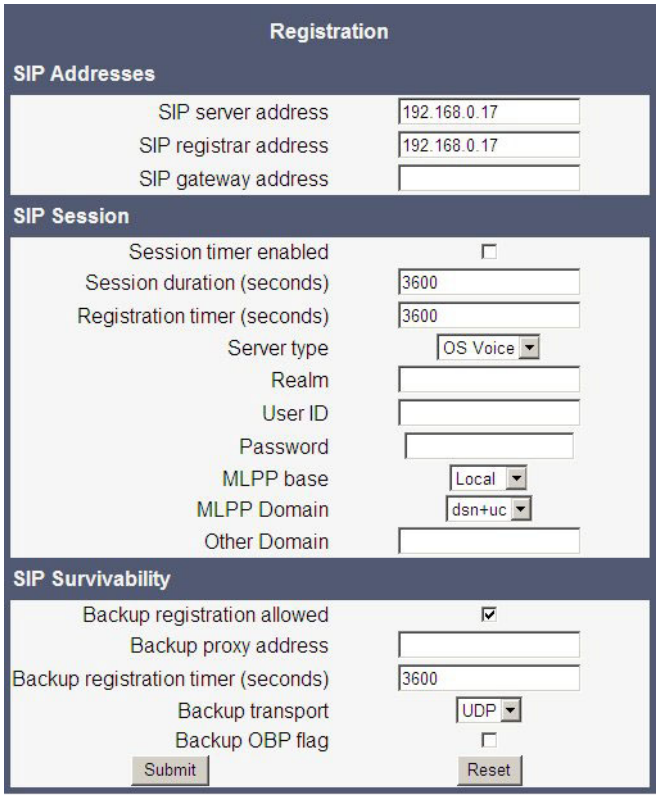
Data required

- **Registration timer (seconds)**: Expiry time of the registration in seconds.
  Default value: 3600.
- **Server type**: Type of server the phone will register to.
  Value range: "Other", "OS Voice", "HiQ8000", "Genesys"
  Default value: "OS Voice"

- **Realm**: Protection domain for authentication.
- **User ID**: User name required for an authenticated registration.
- **Password**: Password required for an authenticated registration.

Administration via WBM

System > Registration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Registration	
|--- SIP Session	
|--- Registration timer	
|--- Server type	
|--- Realm	
|--- User ID	
|--- Password	

3.5.7 SIP Communication

3.5.7.1 Outbound Proxy

If this option is set to "Yes", the phone routes outbound requests to the configured proxy. The outbound proxy will fulfill the task of resolving the domain contained in the SIP request. If "No" is set, the phone will attempt to resolve the domain by itself.

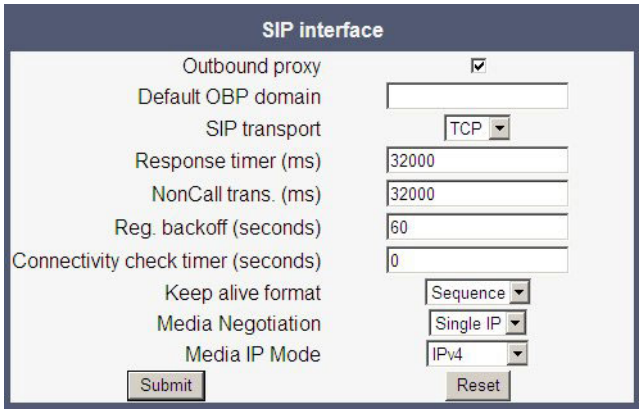
If a **Default OBP domain** (**Outbound Proxy** checkbox) is set and the number or name dialed by the user does not provide a domain, this value will be appended to the name or number. Otherwise, the domain of the outbound proxy will be appended.

Data required

- **Outbound proxy**: Determines whether an outbound proxy is used or not.
  Value range: "Yes", "No"
  Default: "Yes"; when System > Registration > Server type is set to "HiQ8000" (firmware version V3 onwards): "Yes"
- **Default OBP domain**: Alternative value for the domain that is given in the outbound request.

Administration via WBM

System > SIP interface



Administration via Local Phone

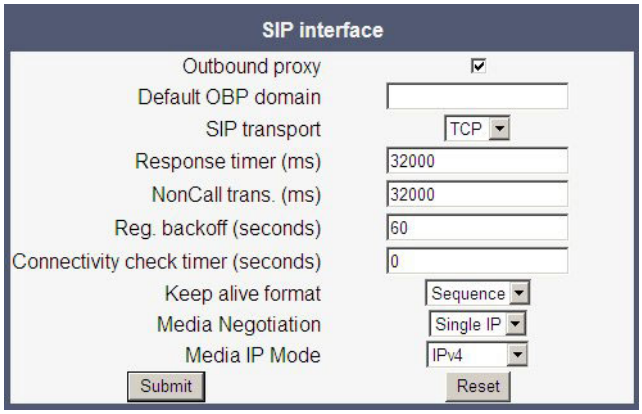
|--- Admin	
|--- System	
|--- SIP Interface	
|--- Outbound proxy	
|--- Default OBP domain	

3.5.7.2 SIP Transport Protocol

Selects the transport protocol to be used for SIP messages. The values "UDP", "TCP", and "TLS" are available. The default is "UDP"; Default when System > Registration > Server type is set to "HiQ8000" (firmware version V3 onwards): "TLS".

Administration via WBM

System > SIP interface



Administration via Local Phone

|--- Admin	
|--- System	
|--- SIP Interface	
|--- SIP transport	

3.5.7.3 Media/SDP

OpenScape Desk Phones support IPv4/IPv6 media address negotiation in SDP using ANAT (Alternative Network Address Types). ANAT allows for for the expression of alternative network addresses (e. g., different IP versions) for a particular media stream.

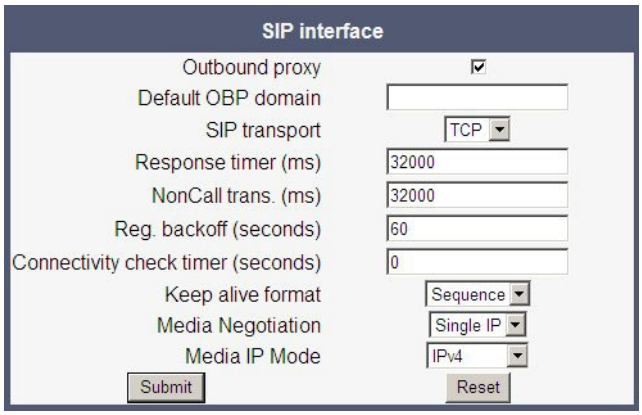
When **Media negotation** is set to "ANAT", ANAT is supported; the phone will re-register with the SIP server and advertise ANAT support in the SIP header. When set to "Single IP", ANAT support is disabled.

> ***INFO:*** If SRTP is enabled, ANAT interworking is only possible if SDES is configured as the key exchange protocol for SRTP (see *Security - General Configuration*).

Media IP mode defines which IP version is to be used for voice transmission. With "IPv4", only IPv4 is used; with "IPv6", only IPv6 is used; with "IPv4_IPv6", both IPv4 and IPv6 can be used, but IPv4 is preferred; with "IPv6_IPv4", both IPv6 and IPv4 can be used, but IPv6 is preferred.

Administration via WBM

System > SIP interface



Administration via Local Phone

|--- Admin	
|--- System	
|--- SIP Interface	
|--- Media negotiation	
|--- Media IP mode	

3.5.8 SIP Session Timer

Session timers provide a basic keep-alive mechanism between 2 user agents or phones. This mechanism can be useful to the endpoints concerned or for stateful proxies to determine that a session is still alive. This is achieved by the phone sending periodic re-INVITEs to keep the session alive. If no re-INVITE is received before the interval passes, the session is considered terminated. Both phones are supposed to terminate the call, and stateful proxies can remove any state for the call.

This feature is sufficiently backward compatible such that only one end of a call needs to implement the SIP extension for it to work.

The parameter **Session timer enabled** determines whether the mechanism shall be used, and **Session duration (seconds)** sets the expiration time, and thus the interval between refresh re-INVITEs.

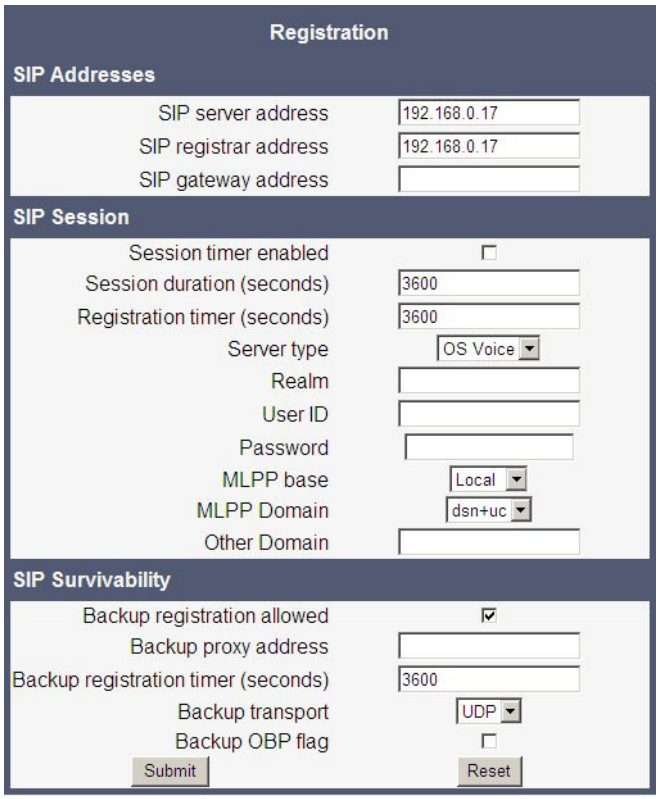
> ***INFO:*** Some server environments support their own mechanism for auditing the health of a session. In these cases, the Session timer must be deactivated. For OpenScape Voice, the Session timer should be deactivated.

Data required

- **Session timer enabled**: Activates or deactivates the session timer mechanism. Value range: "Yes", "No" Default value: "No"
- **Session duration (seconds)**: Sets the expiration time for a SIP session. Default: 3600

Administration via WBM

System > Registration



Administration via Local Phone

└--- Admin	
|--- System	
|--- Registration	
|--- SIP session	
|--- Session timer	
|--- Session duration	

3.5.9 Resilience and Survivability

To allow for stable operation even in case of network or server failure, OpenScape Desk Phones have the capability of switching to a fallback system. The switch-over is controlled by various configurable check and timeout intervals.

Survivability is achieved in two different ways:

1. DNS SRV can be used for enhanced survivability, either in a scenario with a survivability proxy, or in a scenario with multiple primary SIP servers. The DNS -server provides the phone with a prioritized list of SIP servers via DNS SRV. The phone fetches this list periodically from the server, depending on the TTL (time to live) specified for the DNS SRV records.
   To enable DNS SRV requests from the phone, please make the following settings:
   - Specify the IP address of the DNS server that provides the server list via DNS SRV. The web interface path is Network > IP configuration > Primary DNS. For details, see *DNS Servers*.
   - Enable the use of an outbound proxy for routing outbound requests. The web interface path is System > SIP interface > Outbound proxy. For details, see *Outbound Proxy*.
   - Set the SIP gateway port to 0. The web interface path is Network > Port configuration > SIP gateway.
     If the SIP server is to be configured by DNS SRV, set the SIP server port to 0. The web interface path is Network > Port configuration > SIP server. The SIP server address is specified in System > Registration > SIP server address. For details, see *SIP Ports*.
   - As SIP gateway address, enter the DNS domain name for which the DNS SRV records are valid. The web interface path is System > Registration > SIP gateway address.
     If the SIP server is to be configured by DNS SRV, set the mentioned parameter to the DNS domain name for which the DNS SRV records are valid. The SIP server address is specified in System > Registration > SIP server address. For details, see *SIP Addresses*.

   A survivability proxy acts as a relay between the phone and the primary SIP server. Thus, the address of the survivability proxy is specified as gateway or SIP server at the phone (see *SIP Registration*). When the TLS connection

between the survivability proxy and the SIP server breaks down, e. g. because of server failure, the survivable proxy itself acts as a replacement for the primary SIP server. Vice versa, in case the phone can not reach the survivability proxy itself, it will register directly with the primary SIP server, provided that it is specified in the DNS SRV server list.
The survivability proxy notifies the phone whenever the survivability changes, so it can indicate possible feature limitations to the user. Furthermore, to enhance survivability, the phone will be kept up-to-date about the current survivability state even after a restart.
Another way to realize survivability is the use of multiple, geographically separated SIP servers. Normally, the phone is registered with that server that has the highest priority in the DNS SRV server list. If the highest priority server fails to respond to the TLS connectivity check (see *Connectivity Check*), the phone will register with the server that has the second highest priority.

2. Use of a Backup SIP Server. Along with the registration at the primary SIP server, the phone is registered with a backup SIP server. In normal operation, the phone uses the primary server for outgoing calls. If the phone detects that the connection to the primary SIP server is lost, it uses the backup server for outgoing calls. This connection check is realized by 2 timers; for details, see *Response Timer* and *Non-INVITE Transaction Timer*. For configuring the backup server, please refer to *Backup SIP Server*.

INFO: In survivability mode, some features will presumably not be available. The user will be informed by a message in the Call View display.

3.5.9.1 Connectivity Check

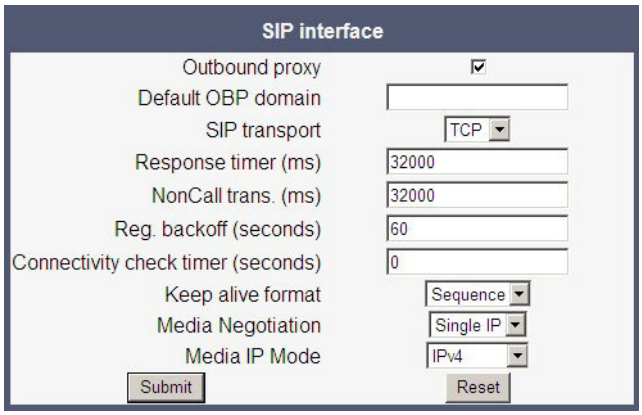
A regular check ensures that the TLS link to the main SIP server is active. When the **Connectivity check timer** is set to a non-zero value, test messages will be sent at the defined interval. If the link is found to be dead, the phone uses DNS SRV to find another SIP server. Certainly, the DNS SRV records must be properly configured in the DNS server.

Value range: 0 (off), and 10 to 3600 sec.

If no other primary SIP server is found via DNS SRV, the phone will switch over to a backup server for making receiving calls. For configuring the backup server, please refer to *Backup SIP Server*.

Administration via WBM

System > SIP interface



3.5.9.2 Response Timer

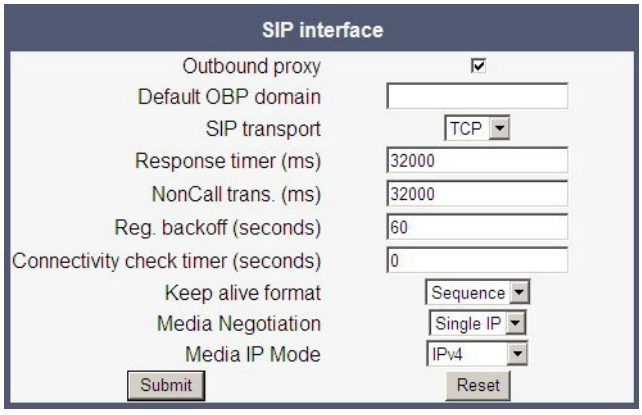
The **Response Timer** resp. **Call trans.** timer is started whenever the phone sends a new INVITE message to the SIP server.

If the call transaction timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If there is no backup server configured, the phone just tidies up internally.

The data is given in milliseconds. The default value is 32 000; for OpenScape Voice, the recommended setting is 3.7 seconds (3700 ms).

Administration via WBM

System > SIP interface



Administration via Local Phone

|--- Admin	
|--- System	
|--- SIP Interface	
|--- Call trans. (ms)	

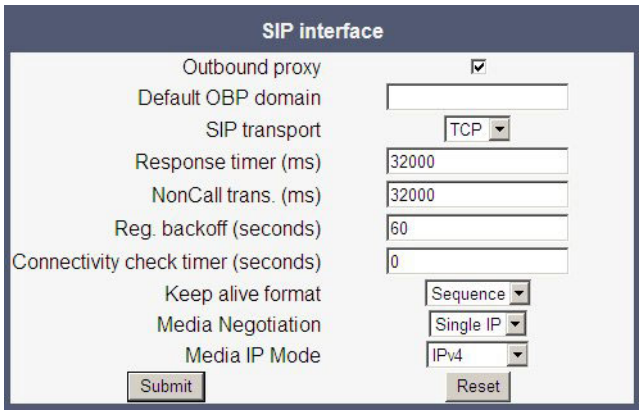
3.5.9.3 Non-INVITE Transaction Timer

The **NonCall trans.** timer is started whenever the phone sends a non-INVITE message to the SIP server. If the timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If no backup server is configured, the phone will just tidy up internally.

The data is given in milliseconds. The default value is 32000; for OpenScape Voice, the recommended setting is 6 seconds (6000 ms).

Administration via WBM

System > SIP interface



Administration via Local Phone

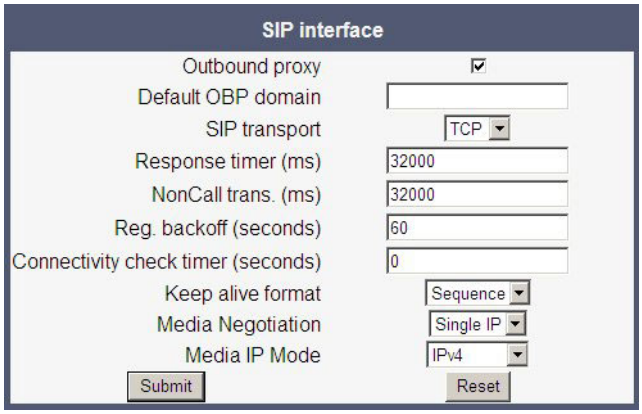
|--- Admin	
|--- System	
|--- SIP Interface	
|--- NonCall transactions (ms)	

3.5.9.4 Maximum Registration Backoff Timer

If a registration attempt should result in a timeout, the phone waits a random time before sending another REGISTER message. The **Reg. backoff (seconds)** parameter determines the maximum waiting time.

Administration via WBM

System > SIP interface



Administration via Local Phone

|--- Admin	
|--- System	
|--- SIP Interface	
|--- Reg. backoff	

3.5.9.5 Backup SIP Server

The **Backup registration allowed** flag indicates whether or not the phone treats the backup proxy server as a SIP registrar. If set to "Yes", the phone tries to register its SIP address with the server whose IP address or hostname is specified by **Backup proxy address**. Once an IP address has been entered, the SIP-UDP Port is opened, even if SIP-TLS is used for the OS Voice connection.

The **Backup registration timer** determines the duration of a registration with the backup SIP server.

The **Backup transport** option displays the current transport protocol used to carry SIP messages to the Backup proxy server.

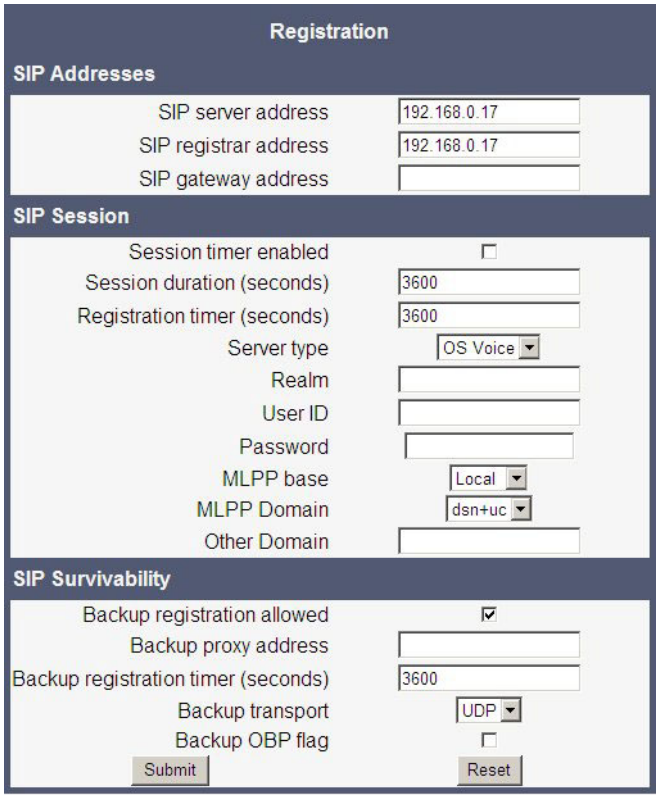
The **Backup OBP flag** indicates whether or not the Backup proxy server is used as an outbound proxy.

Data required

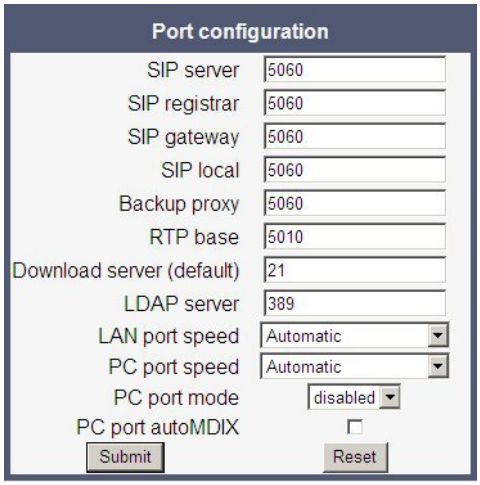
- **Backup registration allowed / Backup registration flag**: Determines whether or not the backup proxy is used as a SIP Registrar.
  Value Range: "Yes", "No"
  Default: "Yes"
- **Backup proxy address**: IP address or hostname of the backup proxy server.
- **Backup registration timer**: Expiry time of the registration in seconds.
  Default: 3600
- **Backup transport**: Transport protocol to be used for messages to the backup proxy.
  Value range: "TCP", "UDP"
  Default: "UDP"
- **Backup OBP flag**: Determines whether or not the backup proxy is used as an outbound proxy.
  Value range: "Yes", "No"
  Default: "No"
- **Network > Port Configuration > Backup proxy**: Port of the backup proxy server.
  Default: 5060

Administration via WBM

System > Registration



Network > Port configuration



Administration via Local Phone

└--- Admin	
|--- System	
|--- Registration	
|--- SIP Session	
|--- SIP Survivability	
|--- Backup registration flag	
|--- Backup proxy address	
|--- Backup transport	
|--- OBP flag	

└--- Admin	
|--- Network	
|--- Port Configuration	
|--- Backup proxy	

3.6 Feature Access

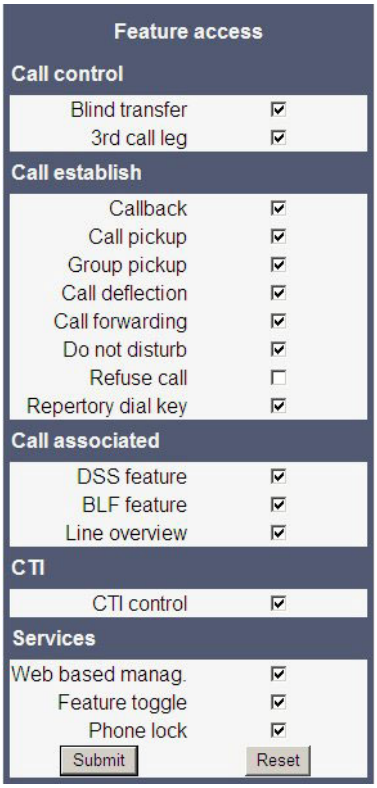
Certain OpenScape Desk Phone features and interfaces can be enabled or disabled:

- Blind Transfer (see *Blind Call Transfer*)
- 3rd Call Leg (consultation from a second call; see *User Manual*)
- Callback Busy (see *Callback* and *Callback URIs*)
- Callback on No Reply (see *Callback* and *Callback URIs*)

- Callback Pause and Resume (see *Pause Callbacks* and *Resume Callbacks*
- Callback Cancel (see *Cancel Callbacks* and *Callback URIs*)
- Call Pickup (see *Directed Pickup*)
- Group Pickup (see *Group Pickup*)
- Call Deflection (see *Deflect a Call*)
- Call Forwarding (see *Call Forwarding*)
- Do Not Disturb (see *Do Not Disturb*)
- Refuse Call (see *Allow Refuse*)
- Repertory Dial Key (see *Repertory Dial*)
- DSS Feature (see *Direct Station Select (DSS)*)
- BLF Feature (see *BLF Key*)
- Line Overview (see *User Manual*)
- CTI Control (see *uaCSTA Interface*)
- Web-Based Management (see *Web-based Management (WBM)*)
- Feature Toggle (see *Hunt Group: Send Busy Status Using Feature Toggle*)
- Phone Lock (see *User Manual*)

Administration via WBM

System > Features > Feature access



└--- Admin	
|--- System	
|--- Features	
|--- Feature access	
|--- Call control	
|--- Blind transfer	
|--- 3rd call leg	

Administration via Local Phone

└--- Admin	
|--- System	
|--- Features	
|--- Feature access	
|--- Call establish	
|--- Callback	
|--- Call pickup	
|--- Group pickup	
|--- Call deflection	
|--- Call forwarding	
|--- Do not disturb	
|--- Refuse call	
|--- Repertory dial key	

└--- Admin	
|--- System	
|--- Features	
|--- Feature access	
|--- Call associated	
|--- Phone book lookups	
|--- DSS feature	
|--- BLF feature	
|--- Line overview	

|--- Admin	
|--- System	
|--- Features	
|--- Feature access	
|--- CTI	
|--- CTI control	

|--- Admin	
|--- System	
|--- Features	
|--- Feature access	
|--- Services	
|--- Web based mang.	
|--- Feature toggle	
|--- Phone lock	

3.7 Feature Configuration

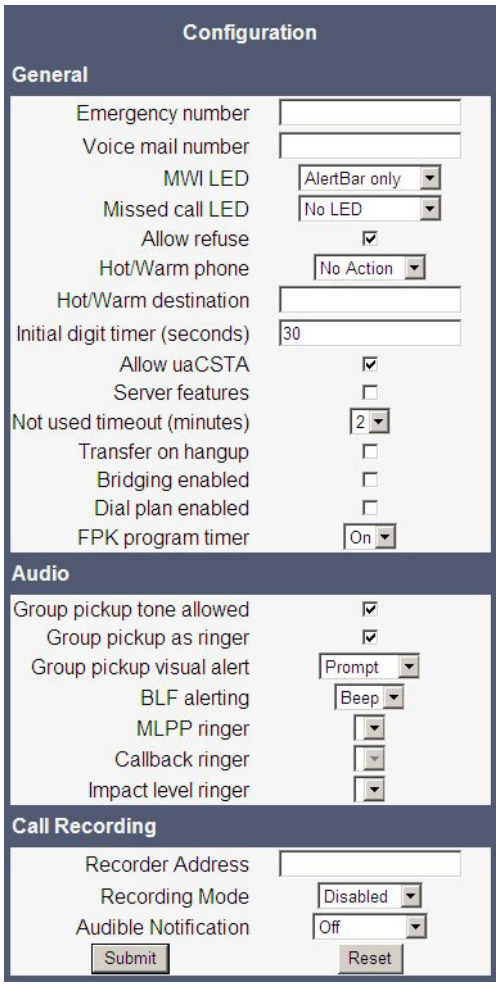
3.7.1 Allow Refuse

This parameter defines whether the **Refuse Call** feature is available on the phone. The possible values are "Yes" or "No". The default is "**No**".

INFO: This parameter can also be configured under System > Features > Feature access (see *Feature Access*).

Administration via WBM

System > Features > Configuration



Administration via Local Phone

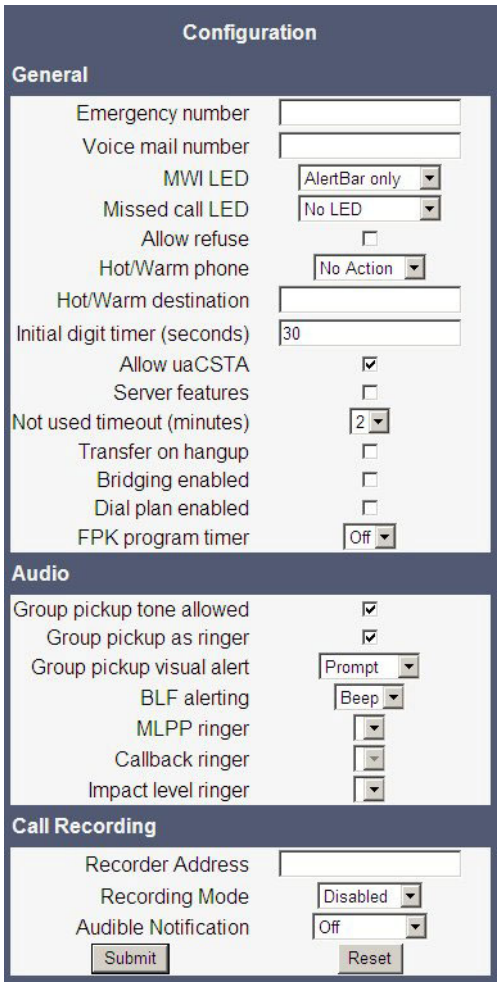
|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Allow refuse	

3.7.2 Hot/Warm Phone

If the phone is configured as hot phone, the number specified in Hot warm destination is dialed immediately when the user goes off-hook. For this purpose, Hot warm phone must be set to Hot phone. If set to Warm phone, the specified destination number is dialed after a delay which is defined in Initial digit timer (seconds) (for details, see *Initial Digit Timer*). During the delay period, the user can dial a number which will be used instead of the hot/warm destination. In addition, the user will be provided with a dial tone during the delay period. With the setting No action, hot phone or warm phone functionality is disabled.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

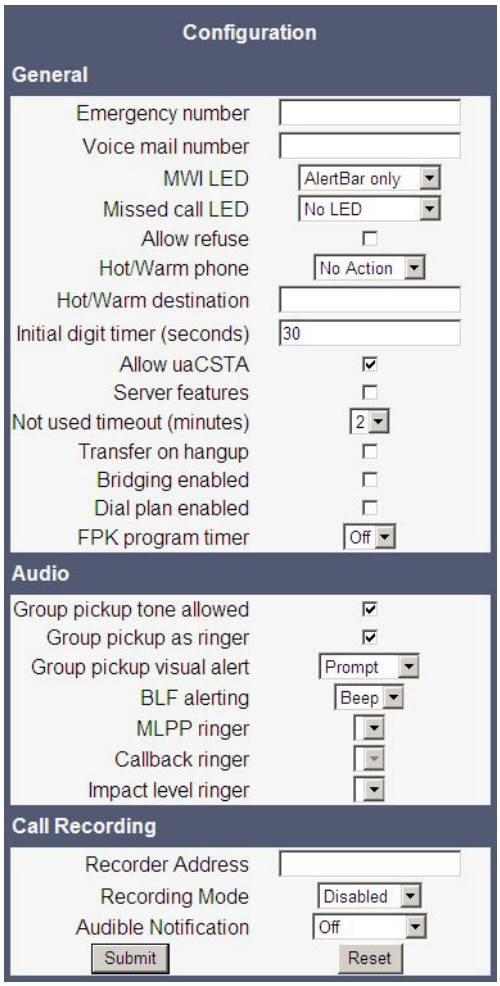
└--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Hot / warm phone	
|--- Hot / warm destination	
|--- Initial digit timer	

3.7.3 Initial Digit Timer

This timer is started when the user goes off-hook, and the dial tone sounds. When the user has not entered a digit until timer expiry, the dial tone is turned off, and the phone changes to idle mode. The **Initial digit timer (seconds)** parameter defines the duration of this time span.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Initial digit timer	

3.7.4 Group Pickup

	This feature is only available when enabled under System > Features > Feature access (see *Feature Access*).

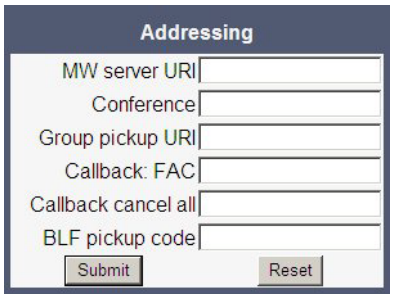
3.7.4.1 Addressing - via Group Pickup URI Feature Code

This feature allows a user to collect a call from any ringing phone that is in the same pickup group. To be a member of a Call Pickup group, the phone must be configured with the corresponding URI of the Call Pickup Group service provided by the server. An example pickup URI is "**3".

Administration via WBM

INFO: The BLF pickup code parameter is only relevant when the phone is connected to an Asterisk server.

System > Features > Addressing



3.7.4.2 Pickup Alert

If desired, an incoming call for the pickup group can be indicated acoustically and visually if **Group pickup visual alert** is configured.

The **Group pickup tone allowed** parameter activates or deactivates the generation of an acoustic signal for incoming pickup group calls. The default is "Yes". If this is activated, **Group pickup as ringer** determines whether the current ring tone or an alert beep is used. If set to "Yes", a pickup group call will be signaled by a short ring tone; the currently selected ringtone is used. If set to "No", a pickup group call will be signaled by an alert tone. The default is "Yes".

Depending on the phone state and the setting for **Group pickup as ringer**, the group pickup tone comes from the loudspeaker, the handset, or the headset. The volumes can be set in the local **User menu**, under **Audio > Volumes**.

The following table shows the group pickup alert behavior for each possible scenario:

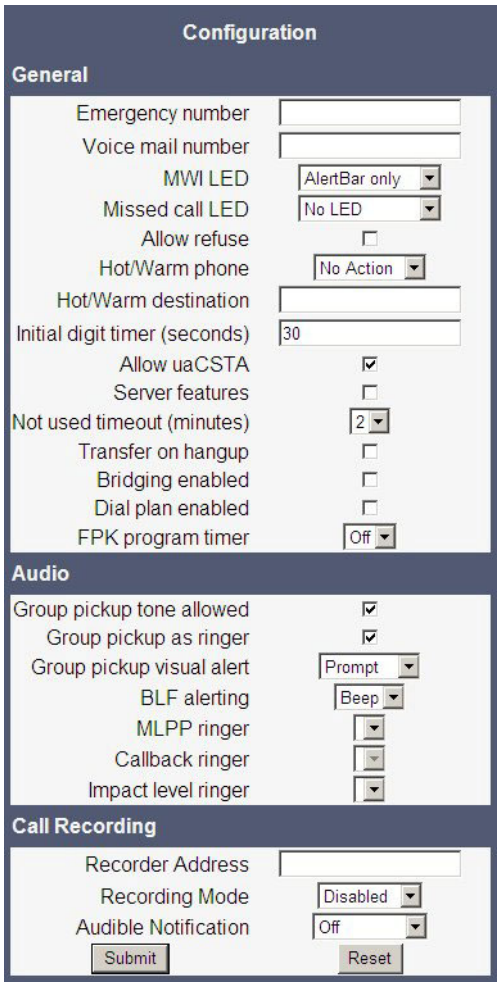
Phone State			Group pickup as ringer=yes	Group pickup as ringer=no
Ringer on	Idle		Ring tone Speaker	Beep Speaker
	In call	Handset	Ring tone Speaker	Beep Handset
		Handset Open listening	Beep Handset and Speaker	Beep Handset and Speaker
		Headset	Ring tone Speaker	Beep Headset
		Headset Open listening	Beep Headset and Speaker	Beep Headset and Speaker
		Hands-free	Beep Speaker	Beep Speaker
Ringer off	Idle		Nothing	Nothing
	In call	Handset	Nothing	Beep Handset
		Handset Open listening	Beep Handset and Speaker	Beep Handset and Speaker
		Headset	Nothing	Beep Headset
		Headset Open listening	Beep Headset and Speaker	Beep Headset and Speaker
		Hands-free	Beep Speaker	Beep Speaker

Group pickup visual alert defines the user action required to accept a pickup call.

- If **Prompt** is selected, an incoming pickup call is signaled by the **Pickup call?** prompt on the display and by the flashing **Pick up** key. As soon as the user goes off-hook or presses the **Speaker** key or the **Headset** key, the pickup call is accepted. Alternatively, the user can press the flashing **Pick up** key (if configured) to accept the call.
- If **Notify** is selected, an incoming pickup call is signaled by the **Pickup call?** prompt on the display and by the flashing **Pick up** key. To accept the call, the user must confirm the alert by pressing the **OK** key or by pressing the flashing **Pick up** key. The user can then either lift the handset or press the **Speaker** key or the **Headset** key to accept the call.
- If **FPK only** (default setting) is selected, an incoming call is signaled only by the flashing **Pick up** key. To accept the call, the user must press the flashing **Pick up** key. The **Pickup call?** prompt is then shown on the display, and the user can either lift the handset or press the **Speaker** key or the **Headset** key to accept the call.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- Audio	
|--- Pickup tone	
|--- Pickup as ringer	
|--- Pickup visual	
|--- BLF alerting	

|--- MLPP ringer	
|--- Callback ringer	
|--- Lower IL ringer	

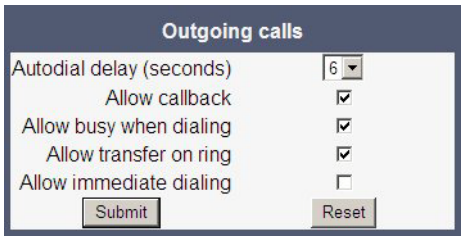
3.7.5 Call Transfer

3.7.5.1 Transfer on Ring

If this function is active, a call can be transferred after the user has dialed the third participant's number, but before the third party has answered the call. This feature is enabled or disabled in the **User menu**. The default is "Yes".

Administration via WBM

(User) Configuration > Outgoing calls



Administration via Local Phone

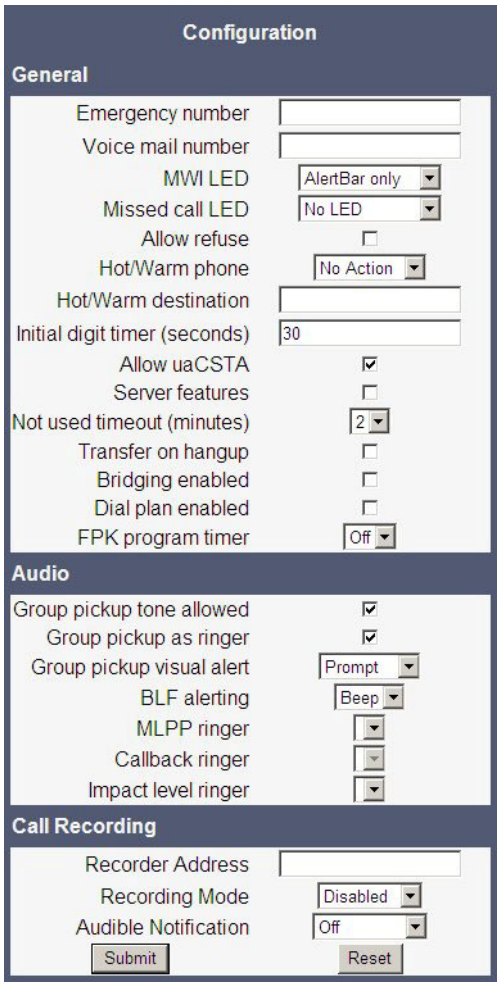
|--- User	
|--- Configuration	
|--- Outgoing calls	
|--- Transfer on ring	

3.7.5.2 Transfer on Hangup

This feature applies to the following scenario: While A is talking to B, C calls A. A accepts the call, so B is on hold and the call between A and C is active. If **Transfer on hangup** is enabled, and A goes on-hook, B gets connected to C. If disabled, C will be released when A hangs up, and A has the possibility to reconnect to B. By default, the feature is disabled.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Transfer on hangup	

3.7.6 Callback URIs

The **Callback** option allows the user to request a callback on certain conditions. The callback request is sent to the SIP server. The Code for callback busy requests a callback if the line is busy, i. e. if there is a conversation on the remote phone. Code for callback no reply applies when the call is not answered, i. e. if nobody lifts the handset or accepts the call in another way. **Callback cancel all** deletes all the callback requests stored previously on the telephone system/SIP server.

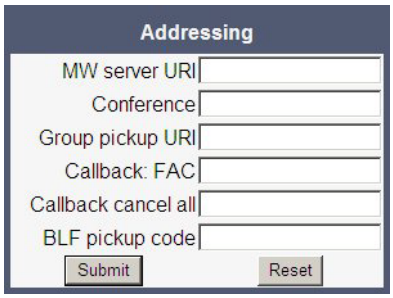
> ***INFO:*** The callback feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Data required

- **Callback: FAC**: Access code that is sent to the server for all kind of Callback .
- **Callback Cancel all**: Access code for canceling all callback requests on the server.

Administration via WBM

System > Features > Addressing



Administration via Local Phone

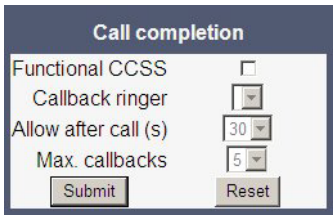
|--- Admin	
|--- System	
|--- Features	
|--- Addressing	
|--- Callback: FAC	
|--- Callback: Cancel all	

3.7.6.1 Call Completion

Used with Asterisk only

Administration via WBM

System > Features > Call Completion



Administration via Local Phone

└--- Admin	
|--- System	
|--- Features	
|--- Call completion	
|--- Functional CCSS	
|--- Callback ringer	
|--- Allow after call (s)	
|--- Max. callbacks	

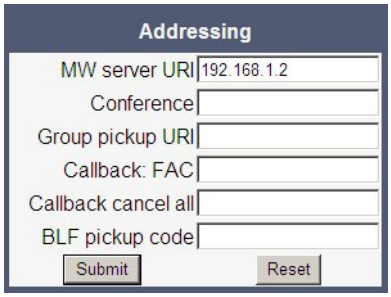
3.7.7 Message Waiting Address

The MWI (Message Waiting Indicator) is an optical signal which indicates that voicemail messages are on the server. Depending on the SIP server / gateway in use, the **Message waiting server address**, that is the address or host name of the server that sends message waiting notifications to the phone, must be configured.

With OpenScape Voice, this setting is not typically necessary for enabling MWI functionality.

Administration via WBM

System > Features > Addressing



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Addressing	
|--- MWI server URI	

3.7.8 Indicate Messages

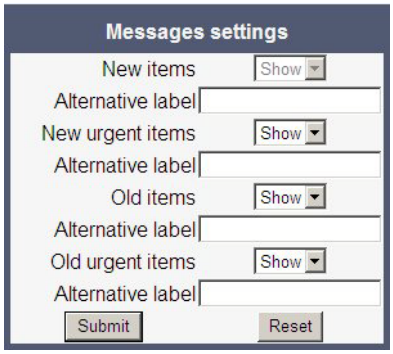
The indication of old and new messages on the display can be configured. There are 4 categories of voicemail messages: new, new urgent, old, and old urgent. For each category, the administrator can define whether the message count is shown or hidden, and set a header for the category.

Data required

- **New items**: Determines whether new items are indicated.
  Fixed Value: "Show".
- **Alternative label**: Label for new items.
- **New urgent items**: Determines whether new urgent items are indicated.
  Value range: "Show", "Hide"
- **Alternative label**: Label for new urgent items.
- **Old items**: Determines whether new urgent items are indicated.
  Value range: "Show", "Hide"
- Alternative label: Label for old items.
- **Old urgent items**: Determines whether old urgent items are indicated.
  Value range: "Show", "Hide"
- **Alternative label**: Label for old urgent items.

Administration via WBM

Local functions > Messages settings



Administration via Local Phone

|--- Admin	
|--- Local functions	
|--- Messages settings	
|--- New items	
|--- Alternative label	
|--- New urgent items	
|--- Alternative label	
|--- Old items	
|--- Alternative label	
|--- Old urgent items	
|--- Alternative label	

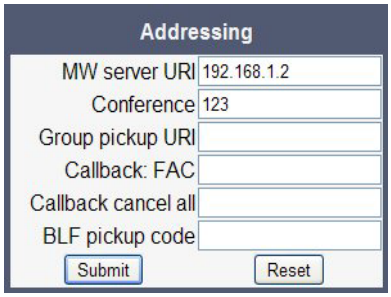
3.7.9 System-Based Conference

The **Conference** URI provides the number/URI used for system based conferences, which can involve 3 to 16 members. This feature is not available with every system.

INFO: It is recommended not to enter the full URI, but only the user part. For instance, enter "123", not "123@<SIP SERVER ADDRESS>". A full address in this place might cause a conflict when OpenScape Voice uses multiple nodes.

Administration via WBM

System > Features > Addressing



3.7.10 Server Based Features

INFO: Please note that the Server features parameter, despite the name similarity, is not related to the Server feature functionality as described in *Server Feature*.

The use of server based call forwarding and server based DND is enabled or disabled here. When phone based DND and phone based call forwarding are to be used, **Server features** must be deactivated. This is the default setting. For using server based Call Forwarding or server based DND, it must be activated.

INFO: Server features is deactivated automatically if System > Registration > Server type (see *SIP Registration*) is set to "HiQ8000".

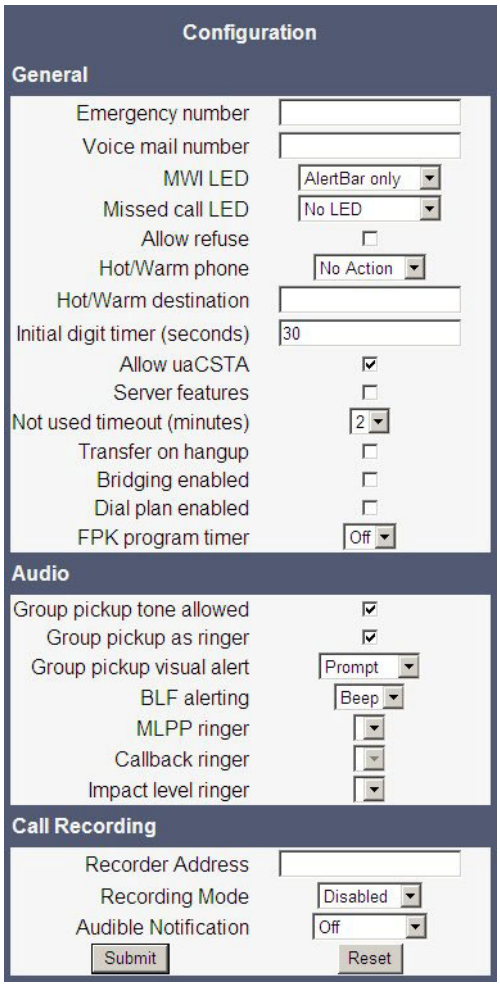
INFO: Before switching Server features on or off, please ensure that both Call Forwarding and DND are not activated. Otherwise, the user will not be able to control the feature any more.

It is recommended to set **Server features** when setting up the phone, and avoid further changes, as possible.

INFO: To enable server based features, uaCSTA must be allowed (see *uaCSTA Interface*).

Administration via WBM

System > Features > Configuration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Server features	

3.7.11 uaCSTA Interface

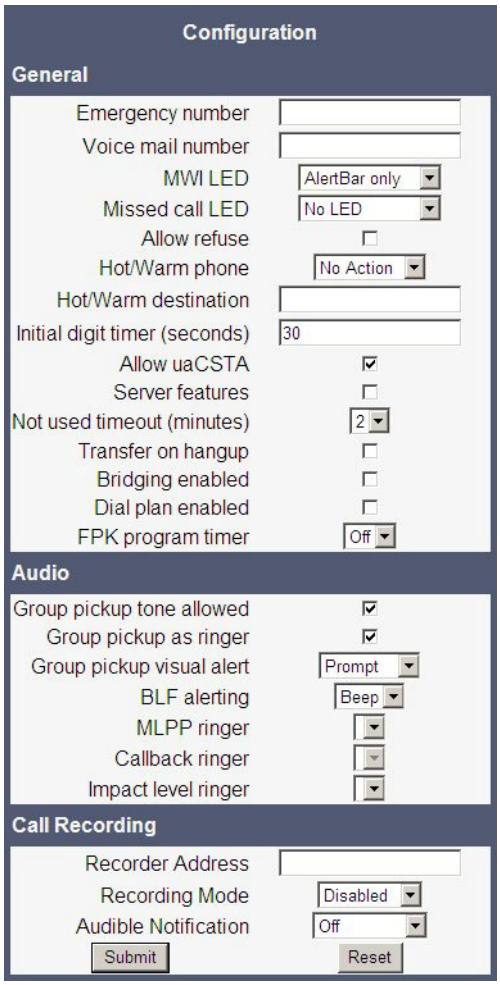
User Agent CSTA (uaCSTA) is a limited subset of the CSTA protocol, which allows external CTI applications to interact with the phone.

> ***INFO:*** Access to the users “CTI calls” menu in User > Configuration > Incoming Calls can be allowed or disallowed (see *Feature Access*).

If **Allow uaCSTA** is enabled, applications which support the uaCSTA standard will have access to the OpenScape Desk Phone. The default is "Yes".

Administration via WBM

System > Features > Configuration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Allow uaCSTA	

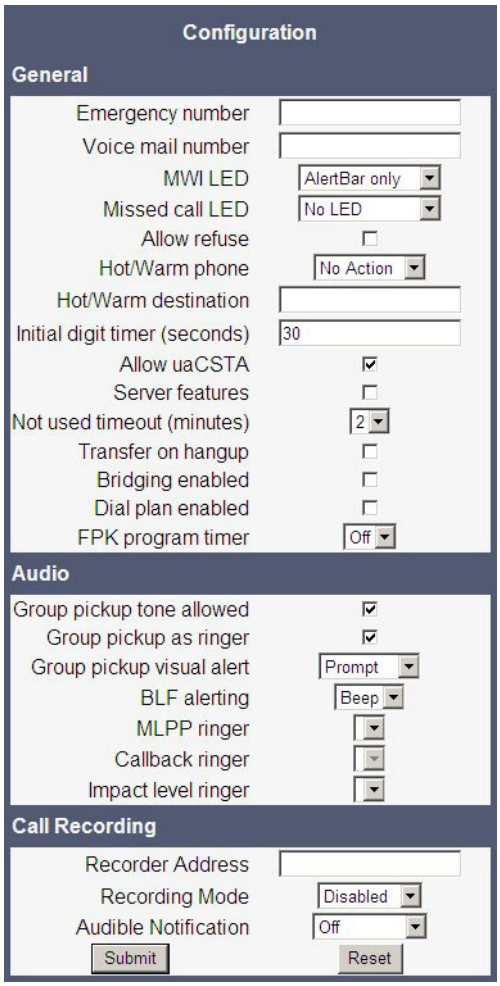
3.7.12 Local Menu Timeout

The timeout for the local **User** and **Admin** menu is configurable. When the time interval is over, the menu is closed and the administrator/user is logged out. The timeout may be helpful in case a user does a long press on a line key unintentionally, and thereby invokes the key configuration menu. The menu will close after the timeout, and the key will return to normal line key operation. The timeout ranges from 1 to 5 minutes. The default value is 2.

INFO: The current position in the **User** or **Admin** menu is kept in case the user/admin has exited the menu, e.g. for receiving a call. Thus, if the user/admin re-enters the menu, he/she is directed to exactly that submenu, or parameter, which he/she had been editing before.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Not used timeout	

3.7.13 Call Recording

Call recording is possible for OpenScape Desk Phones using an "ASC Voice Recorder". The implementation is similar to a local conference, with the recording device acting as the third conference member. To start recording, the phone calls the recording device and provides it with the mixed audio data. Unlike a true local conference, the call leg used for recording can not transport audio from the recording device to the phone.

With the **Call recording mode/Recording mode** parameter, the behavior of the feature is determined:

- "Disabled": Recording is not possible.
- "Manual": The user starts and stops recording manually using the menu or a free programmable key.
- "Auto-start": The recording starts automatically; besides, the user can stop and start the recording manually.
- "All calls": The recording starts automatically for all recordable calls; the user can not stop or start the recording manually.

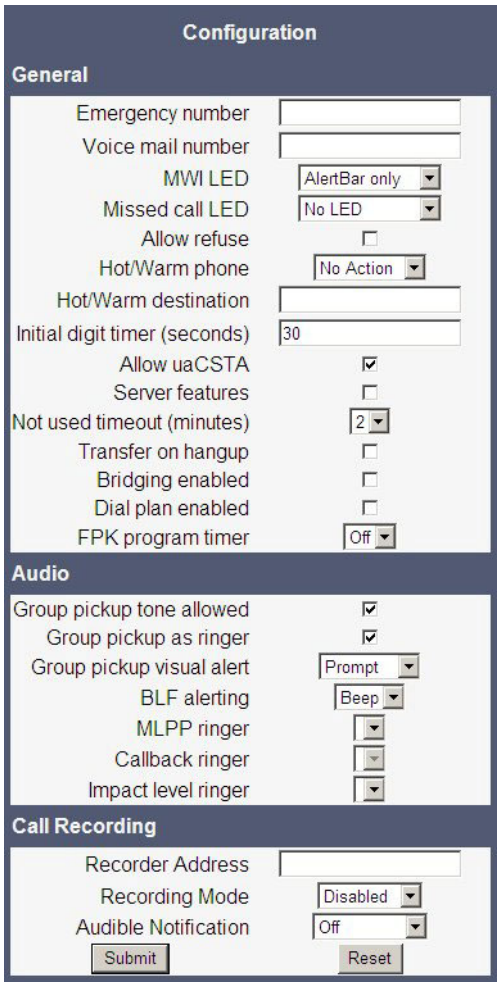
The **Audible indication/Audible notification** parameter determines if and how the parties in a call are informed when a call is being recorded:

- "Off": No audible indication is given.
- "Single-shot": A single audible indication is given when recording commences or resumes.
- "Repeated": An audible indication is given when recording commences or resumes, and repeated periodically during the recording.

With the **Recorder address/Recorder number** parameter, the SIP address of the call recorder is specified.

Administration via WBM

System > Features > Configuration



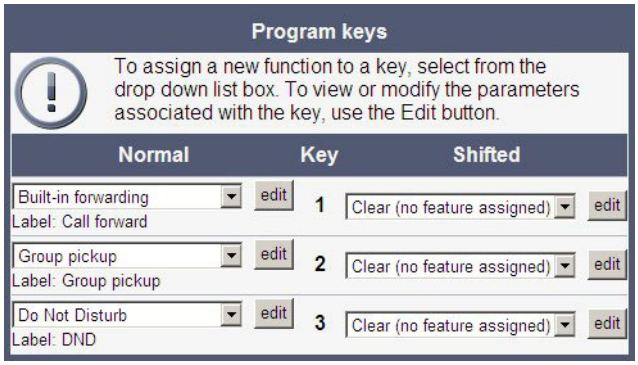
Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- Call recording	
|--- Recorder number	
|--- Recording mode	
|--- Audible notification	

3.8 Free Programmable Keys

OpenScape Desk Phones feature free programmable keys (FPKs) which can be associated with special phone functions. The program keys can be accessed and configured via the WBM or via the Local Phone, as described in *3.8.1 How to Configure Free Programmable Keys (FPKs)*.

> ***INFO:*** To assign a new function to a key, select a function from the drop down list. To view or modify the parameters associated with the key, use the **Edit** button. Click **Submit** to save your changes.



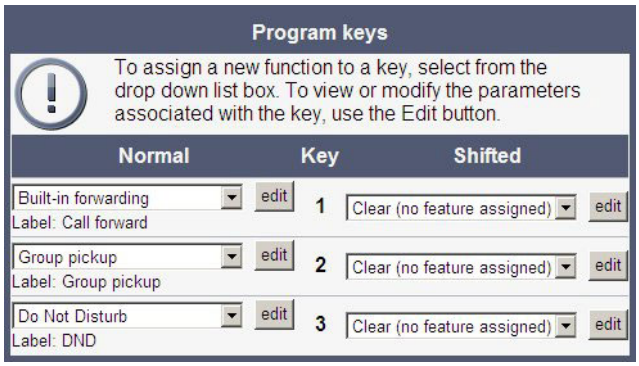
3.8.1 How to Configure Free Programmable Keys (FPKs)

Prerequisites

- Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. The different methods are described below.

Configuring FPKs via WBM

- In the WBM **Administrator** pages, navigate to **System > Features > Program keys**. To assign a new function to a key, select a function from the drop down list. To view or modify the parameters associated with the key, use the **Edit** button. Click **Submit** to save your changes.



OR

- In the WBM **User** pages, navigate to **Phone > Program keys**. To assign a new function to a key, select a function from the drop down list. To view or modify the parameters associated with the key, use the **Edit** button. Click **Submit** to save your changes.

Configuring FPKs on the Local Phone

- In the local phone´s **User** menu, navigate to **User > Phone > Program keys** and press the key to be programmed. Use the navigation keys to select a function and to view or modify the parameters associated with the key. Select **Save&exit** and press **OK** to save your changes.

OR

- At the phone, press and hold the key to be programmed for a few seconds ("long press") until the key´s LED lights up, then use the navigation keys to select a function and to view or modify the parameters associated with the key. Select **Save&exit** and press **OK** to save your changes.

> ***INFO:*** The "long press" feature is disabled by default. It can be enabled by activating the FPK program timer via System > Features > Configuration > (General >) FPK program timer - see *3.8.2 How to Enable "Long Press" for Free Programmable Keys*.

3.8.2 How to Enable "Long Press" for Free Programmable Keys

Prerequisites

- At the phone, the configuration menu for a specific programmable key is called by a long press on the related key.

  INFO: The "long press" feature is disabled by default. It can be enabled by activating the FPK program timer via Administration > System > Features > Configuration > (General >) FPK program timer. When this parameter is disabled, it is not possible to enter the programming mode by long key press. However, the other methods for key programming remain enabled. For keyset and DSS functionality, please refer to *Multiline Appearance/Keyset*.

- The "long press" feature can be enabled or disabled by setting the **FPK program timer** parameter to **On** (enabled) or **Off** (disabled). This can be done either via the WBM **Administrator** pages or via the local phone´s **Admin** menu, as described below.

Step by Step

› In the WBM **Administrator** pages, navigate to **System > Features > Configuration** and set the FPK program timer to **On** or **Off**. Click **Submit** to save your changes.

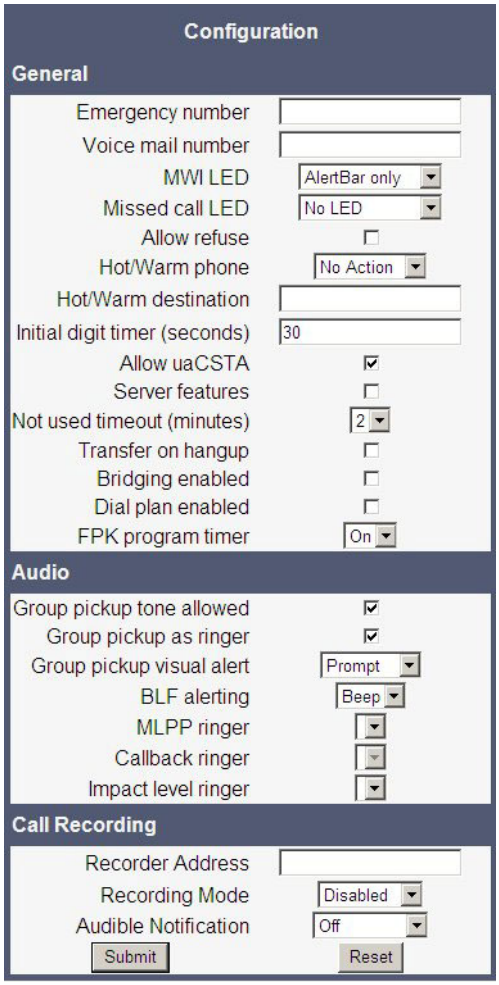
OR

› In the local phone´s **Admin** menu, navigate to **System > Features > Configuration > General > FPK program timer** and set the value to **On** or **Off**. Select **Save&exit** and press **OK** to save your changes.

On your phone, you can now activate the programming mode of a specific programmable key by a long key press on the related key.

Example: Administration via WBM

System > Features > Configuration



Example: Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- FPK prog. timer	

3.8.3 Clear (no feature assigned)

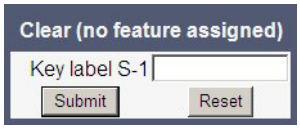
The **Clear (no feature assigned)** function is used as the default placeholder for unallocated program keys.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys



3.8.4 Selected Dialing

On key press, a pre-defined call number is called.

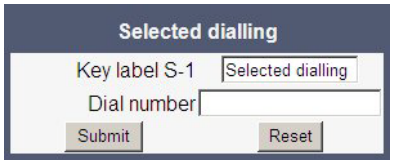
The call number defined in the Dial number parameter is dialed on key press.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Selected dialling



3.8.5 Repeat Dialing

On key press, the call number that has been dialed lastly is dialed again.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Repeat dialling

3.8.6 Call Forwarding

This key function controls phone based call forwarding. If forwarding is enabled, the phone will forward incoming calls to the predefined call number, depending on the current situation.

INFO: To use phone based call forwarding, Server features must be switched off (see *Server Based Features*).

INFO: This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Administration via WBM

System > Features > Program keys > Forwarding

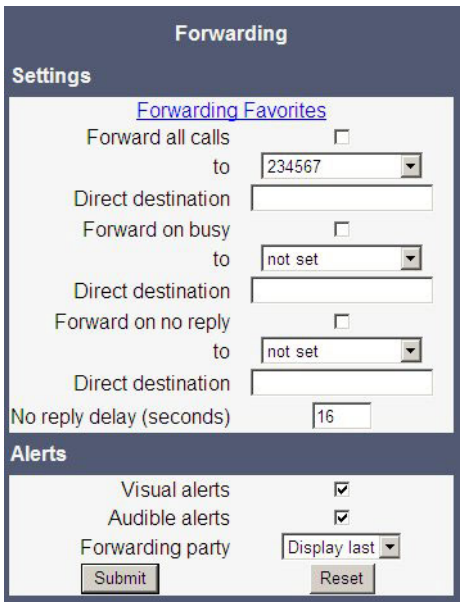
The Forwarding type parameter determines the forwarding behavior.

- If **All calls** is selected, any incoming call will be forwarded.

- If **On no reply** is set, the call will be forwarded when the user has not answered within a specified time span.

  INFO: The time span can be configured via WBM User pages or via the local phone, but only in case of local call forwarding (Server feature disabled), otherwise **No reply delay (seconds)** is not offered.

  In the WBM **User** pages, this feature is configured via **Configuration > Incoming calls > Forwarding > No reply delay (seconds)**.



- If **On busy** is selected, incoming calls will be forwarded when the phone is busy.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

3.8.7 Ringer Off

Turns off the ring tone. Incoming calls are indicated via LEDs and display only.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Ringer off

3.8.8 Hold

The call currently selected or active is put on hold.

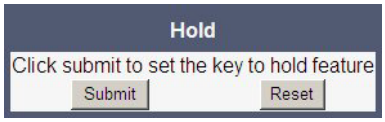
A held call can be retrieved by pressing the key a second time.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Hold



3.8.9 Alternate

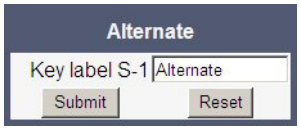
Toggles between two calls; the currently active call is put on hold.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Alternate



3.8.10 Blind Call Transfer

A call is transferred without consultation, as soon as the phone goes on-hook or the target phone goes off-hook.

> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Blind transfer

3.8.11 Join Two Calls

Call transfer, applicable when there is one active call and one call on hold. The active call and the held call are connected to each other, while the phone that has initiated the transfer is disconnected.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Transfer

3.8.12 Deflect a Call

On key press, an incoming call is deflected to the specified destination.

> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

The target destination is defined in the **Destination** parameter field.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Deflect

3.8.13 Shift Level

Shift the level for the programmable keys. When activated, the functions assigned to the shifted level are available on the keys.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Shift

3.8.14 Phone-Based Conference

Establishes a three-party conference from an active call and held call.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Conference

3.8.15 Accept Call via Headset (OpenScape Desk Phones)

On key press, an incoming call is accepted via headset.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Headset

3.8.16 Do Not Disturb

If this feature is activated, incoming calls will not be indicated to the user.

> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Do Not Disturb

3.8.17 Group Pickup

On key press, a call for a different destination within the same pickup group is answered.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Group pickup

3.8.18 Repertory Dial

This feature is similar to the selected dialing function, but additionally, special calling functions are possible.

> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

To configure the feature, enter the desired number and/or function into the **Dial string** parameter field. The following call functions are available:

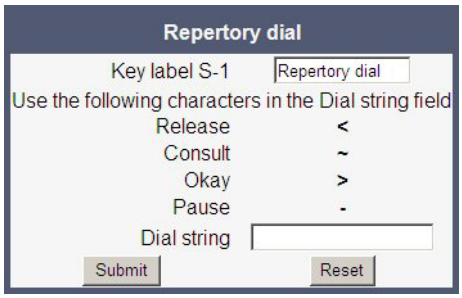
- "<" (Release) - disconnect a call.
- "~" (Consult) - start a consultation call. Example: "~3333>"
- ">" (Okay) (preceded by a call number) - start a call. Example: "3333>"
- "-" (Pause) - enter a pause, e. g. for exit-code or international dialing. Example: "0-011511234567>"

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Repertory dial



3.8.19 Hunt Group: Send Busy Status Using Feature Toggle

This feature is relevant for hunt groups. If the user is a member of a hunt group and wants another member of the hunt group to pick up an incoming call, he can signal Busy status using the **Feature toggle** function.

> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

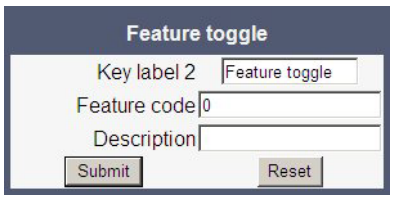
The **Feature code** parameter is the OpenScape Voice code for Busy status. In the **Description** field, an appropriate description for the feature can be entered.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Feature toggle



3.8.20 Mobile User Logon

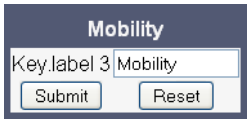
The mobility feature enables users to transfer their personal settings, such as their key layout, or personal phonebook, from one phone to another. The data is stored and managed by the DLS (Deployment Service).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Mobility



3.8.21 Directed Pickup

This feature enables the user to pick up a call which is ringing at another phone. On pressing the key, a menu opens which requests the call number of the target phone.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Directed pickup

3.8.22 Callback

When the remote phone called is busy and does not reply, the user can send a callback request to the server by pressing this key.

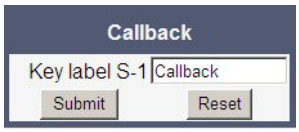
> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Callback



3.8.23 Cancel Callbacks

With this function, the user can cancel all pending callback requests on the server.

> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Cancel callbacks

3.8.24 Pause Callbacks

With this function, the user can pause the execution of all pending callback requests.

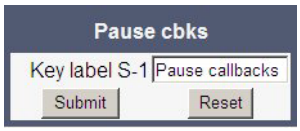
> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Pause callbacks



3.8.25 Resume Callbacks

With this function, the user can resume the execution of all pending callback requests.

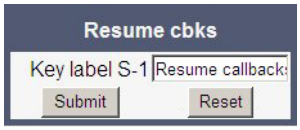
> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Resume callbacks



3.8.26 Consultation

When the phone is engaged in an active call, this function opens a dialing menu to make a consultation call.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Consultation

3.8.27 Call Waiting

Enables or disables the call waiting feature. If enabled, calls from a third party are allowed during an active call.

> ***INFO:*** The Call Waiting feature cannot be disabled if System > Registration > Server type (see *SIP Registration*) is set to "HiQ8000".

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Call waiting

3.8.28 Call Recording

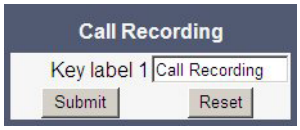
Starts or stops call recording (for configuring call recording, see *Call Recording*).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Call Recording



3.8.29 Auto Answer With Zip Tone

This feature is primarily designed for call centers. If activated, and a headset is used, the phone will automatically accept incoming calls without ringing and without the necessity to press a key. Moreover, additional signaling information from OpenScape Voice is not required.

To indicate a new call to the user, a zip tone is played through the headset when the call is accepted.

> ***INFO:*** The feature is available for OpenScape Desk Phones which provide a headset jack; it only operates if the headset is plugged in. In case the key for feature activation has been pressed before the headset is connected, the feature will be automatically activated when the headset is plugged in.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > AICS Zip tone

3.8.30 Server Feature

Invokes a feature on the SIP server. The status of the feature can be monitored via the LED associated to the key.

> ***INFO:*** This function is intended primarily for operation with an Asterisk SIP server. For details, please refer to the *Administration Manual for OpenScape Desk Phones on Asterisk*.

3.8.31 BLF Key

This function offers the possibility to monitor another extension, and to pick up calls for the monitored extension.

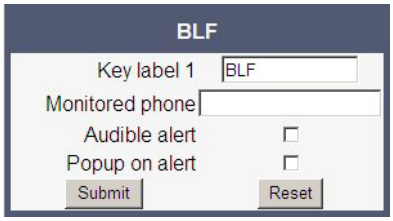
> ***INFO:*** This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

> ***INFO:*** This function is intended primarily for operation with an Asterisk SIP server. For details, please refer to the Administration Manual for OpenScape Desk Phones on Asterisk.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM



3.8.32 Send URL Request via HTTP/HTTPS

With this function, the phone can send a specific HTTP or HTTPS request to a server. The function is available at any time, irrespective of registration and call state. Possible uses are HTTP-controlled features on the system, or functions on a web server that can only be triggered by HTTP/HTTPS request, e. g. login/ logout for flexible working hours.

- The **Protocol** parameter defines whether HTTP or HTTPS is to be used for sending the URL to the server.
- The **Web server address** is the IP address or DNS name of the remote server to which the URL is to be sent.
- The **Port** is the target port at the server to which the URL is to be sent.
- The **Path** is the server-side path to the desired function, i. e. the part of the URL that follows the IP address or DNS name. Example: webpage/ checkin.html
- In the **Parameters** field, one or more key/value pairs in the format `"<key>=<value>"` can be added to the request, separated by an ampersand (&).
  Example: `phonenumber=3338&action=huntGroupLogon`

  INFO: The question mark will be automatically added between the path and the parameters. If a question mark has been entered at the start of the parameters, it will be stripped off automatically.

- The **Method** parameter determines the HTTP method to be used, which can either be GET or POST. If GET is selected, the additional parameters (Parameters) and the user id/password (Web server user ID/Web server password) are part of the URL. If POST is selected, these data form the body of the message.

- In case the web server requires user authentication, the parameters **Web server user ID** and **Web server password** can be used. If not null, the values are appended between the server-side path (**Path**) and the additional parameters (**Parameter**).
- If the **LED controller URI** is given, the LED associated with this key indicates the state of the call number or SIP URI specified, provided the SIP server sends a notification:
  - Busy notification: LED is glowing.
  - Ringing notification: LED is blinking.
  - Idle notification (state=terminated): LED is dark.

  INFO: When assigning the function described here to the release key, please consider that this key has no LED. *Not supported on IP 35G.

- If the **Push support** parameter is activated, the LED is controllable by a combination of an HTTP push request and an XML document. For further information, see the *XML Applications Developer's Guide*.

  INFO: If you want to use the HTTP push solution, please ensure that the LED controller URI field is empty. Otherwise, the phone will only use the SIP mechanism for LED control, and ignore the push request.

- The **Symbolic name** is used to assign a push request from the application server to the appropriate free programmable key resp. fixed function key. This value must be unique for all keys involved.

Data required

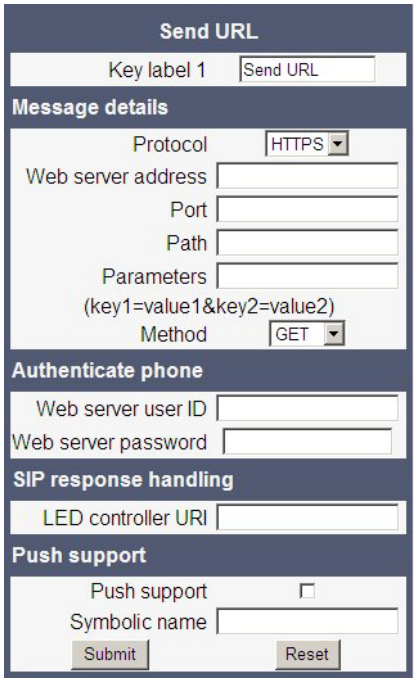
- **Key label <n>**: Label for the key.
- **Protocol**: Transfer protocol to be used. Value range: "HTTP", "HTTPS"
- **Web server address**: IP address or DNS name of the remote server.
- **Port**: Target port at the server.
- **Path**: Server-side path to the function.
- **Parameters**: Optional parameters to be sent to the server.
- **Method**: HTTP method used for transfer. Value range: "GET", "POST"
- **Web server user ID**: User id for user authentication at the server.
- **Web server password**: Password for user authentication at the server.
- **LED controller URI**: Indicates the state of the call number specified.
- **Push support**: Enables or disables LED control by push requests from the server.
- **Symbolic name**: Assigns a push request to the appropriate free programmable key resp. fixed function key.

Administration via WBM

System > Features > Program keys > Send URL

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.



3.8.33 Built-in Forwarding

As a programmable key function, this is relevant for OpenScape Desk Phones which have no fixed forwarding key.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Built-in forwarding

3.8.34 2nd Alert

This function allows for monitoring and accepting a second incoming call. When a call is ringing while the user is dialing, the LED will light up. As soon as the user presses the key, information about the incoming call is presented, and the user can accept the call. If a call is ringing, and another call starts ringing shortly after, the LED will light up, and the user has the possibility to toggle between these calls via key press.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys

3.8.35 Show phone screen

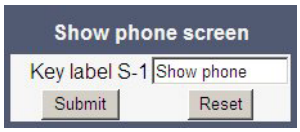
On pressing this key, the phone display switches to call view mode (idle display).

Use the **Key label <key number>** field to define or change the name (label) of the key.

Program keys can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Show phone screen



3.9 Preset Function Keys

The OpenScape Desk Phone IP 35G telephone comes with three programmable lit keys, preset to the following factory settings:

- Forward
- Call Pick Up
- Do Not Disturb (DND)

The Free Programmable Keys (FPKs) can be programmed on two separate levels (Normal and Shift level) but if you reset the phone, the keys in the first level will be reset to the default factory settings.

> ***INFO:*** To use the second (shifted) level, a Shift key is necessary to switch between the two levels. Therefore, 1 of 3 FPKs needs to be programmed as Shift key, and only 2 FPKs remain available for other functions.

3.10 Fixed Function Keys

For the **Conference** call key, the **Transfer** key, and the **Hold** key, specific SIP or HTTP based functions can be defined. If you reset the phone, these three keys will be reset to the default factory settings.

The other fixed function keys (**Messages, Settings, Speaker, Transfer, Headset, Vol.+, Vol.- and Mute**) cannot be programmed with specific functions.

Administration via WBM

In the WBM **Administrator** pages, navigate to **System > Features > Fixed keys**. To assign a new function to a key, select a function from the drop down list. To view or modify the parameters associated with the key, use the **Edit** button. Click **Submit** to save your changes.

3.11 Multiline Appearance/Keyset

A phone that has more than one line associated to it, and therefore works as a multiline phone, is referred to as "keyset". The lines are assigned to the phone by setting up a separate line key for each line.

The multiline appearance feature allows for multiple lines to be assigned to a keyset and for a line to be assigned to multiple keysets. This feature requires configuration in OpenScape Voice and in the telephone, and is particularly useful for executive-assistant arrangements.

In order to configure the phone as a keyset, it is required to

- use an outbound proxy (System > SIP interface > Outbound proxy, see *Outbound Proxy*), and
- set the server type to "OS Voice" (System > Registration > Server type, see *SIP Registration*).

For each keyset, a Primary Line/Main DN is required. The primary line is the dialing number for that keyset.

There are two types of line:

- **Private line**: A line with restricted line status signaling towards OSV.
- **Shared line**: A line that is shared between keysets.

3.11.1 Line Key Configuration

WBM Path: System > Features > Program keys

INFO: Primary lines can only be configured on keys 1 to 3, or 1 to 2 if a Shift key is needed. This ensures that the lines are still accessible when the user migrates to a different phone with fewer keys via the mobility feature.

A line corresponds to a SIP address of record (AoR), which can have a form similar to an E-mail address, or can be a phone number. It is defined by the **Address** parameter. For registration of the line, a corresponding entry must exist on the SIP server resp. the SIP registrar server.

A label can be assigned to the line key by setting its **Key label**.

Every keyset must necessarily have a line key for the primary line. To configure the key of the primary line, set **Primary line** to "true".

If **Ring on/off** is checked, the line will ring when an incoming call occurs, and a popup will appear on the display. If the option is not checked, the incoming call will be indicated only by the blinking of the key's LED. If it is desired that the line ring with a delay, the time interval in seconds can be configured by **Ring delay**.

When the user lifts the handset in order to initiate a call, the line to be used is determined by selection rules. To each line, a priority is assigned by the **Selection order** parameter. A line with the rank 1 is the first line to be considered for use. If more than one line have the same rank, the selection is made according to the key number. Note that **Selection order** is a mandatory setting; it is also relevant to the **Terminating line preference**, as well as to other functions.

The **Address** (Address of Record) parameter is the phone number resp. SIP name corresponding to the entry in the SIP registrar at which the line is to be registered.

INFO: For the configuration of line keys, the use of the DLS (Deployment Service) is recommended. For operating the DLS, please refer to the DLS user's guide. Alternatively, the web

interface or the local menu can be used. Note that the creation of a new line key and the configuration of some parameters can not be accomplished by the phone's local menu.

Generally, it is advisable to restrict the user's possibilities to modify line keys. This can be achieved solely by the DLS. For further instructions, see the *DLS Administration Guide*.

The **Realm**, a protection domain used for authenticated access to the SIP server, works as a name space. Any combination of user id and password is meaningful only within the realm it is assigned to. The other parameters necessary for authenticated access are **User Identifier** and **Password**. For all three parameters, there must be corresponding entries on the SIP server.

The **Shared type** parameter determines whether the line is a shared line, i. e. shared with other endpoints, or a private line, i .e. available exclusively for this endpoint. A line that is configured as primary line on one phone can be configured as secondary line on other phones.

INFO: Shared lines are not available if System > Registration > Server type (see *3.5.6 SIP Registration*) is set to "HiQ8000".

When **Allow in overview** is set to "Yes", the line will be visible in the line overview on the phone's display.

INFO: Line overview can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

If a line is configured as hot line, the number indicated in Hot warm destination is dialed immediately when the user goes off-hook. This number is configured in the User menu under Configuration > Keyset > Lines > Hot/warm destination. To create a hot line, Hot warm action must be set to "hot line". If set to "Warm phone", the specified destination number is dialed after a delay which is defined in Initial digit timer (seconds) (for details, see *Initial Digit Timer*). During the delay period, it is possible for the user to dial a different number which will be used instead of the hot/warm line destination. In addition, the user will be provided with a dial tone during the delay period. With the setting "No action", the line key will not have hot line or warm line functionality.

Data required

- **Key label <n>**: Set the label of the line key with the key number <n>.
  Default: "Line"
- **Primary line**: Determines whether the line is the primary line.
  Value range: "Yes", "No"
  Default: "No"
- **Ring on/off**: Determines whether the line rings on an incoming call.
  Value range: "On", "Off"
  Default: "On"

- **Ring delay (seconds)**: Time interval in seconds after which the line starts ringing on an incoming call.
  Default: 0
- **Selection order**: Priority assigned to the line for the selection of an outgoing line.
  Default: 0
- **Address**: Address/phone number which has a corresponding entry on the SIP server/registrar.
- **Realm**: Domain wherein user id and password are valid.
- **User Identifier**: User name for authentication with the SIP server.
- **Password**: Password for authentication with the SIP server.
- **Shared type**: Determines whether the line is a shared line (shared by multiple endpoints) or a private line (only available for this endpoint).
  Value range: "shared", "private", "unknown".
  Default: "shared"
- **Allow in Overview**: Determines whether the line appears in the phone's line overview.
  Value range: "Yes", "No"
  Default: "Yes"
- **Hot warm action**: Determines if the line is a regular line, a hot line, or a warm line.
  Value range: "No action", "hot line", "warm line"
- **Hot warm destination**: The destination to be dialed from the hot/warm line when the user goes off-hook.

INFO: A new line key can only be added by use of the WBM or, preferably, the DLS. Once a line key exists, it can also be configured via the local menu.

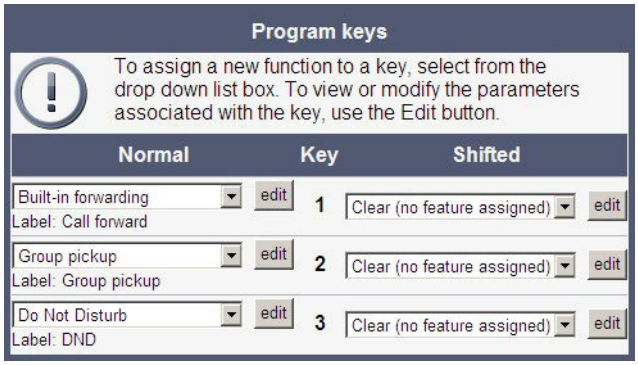
3.11.2 How to Configure Line Keys for Keyset Operation

Administration via WBM

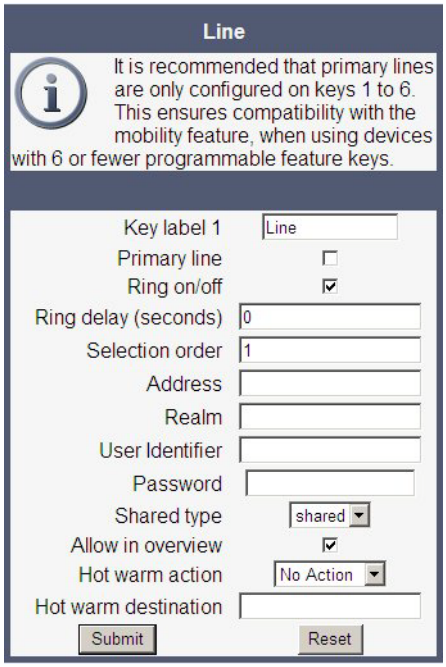
System > Features > Program keys

Step by Step

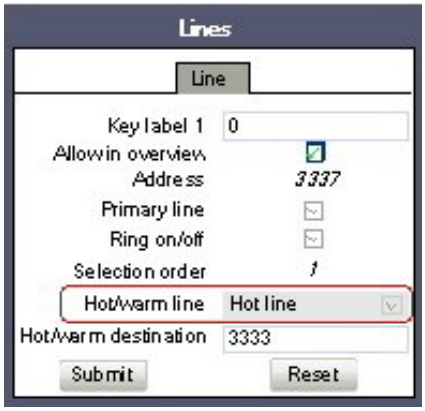
1) Invoke the **Program keys** dialog and select **Line** in the drop down menu of the key you want to configure. Next, click the **edit** button.



2) In the **Line** dialog, set the specific parameters for the line key.



3) (Only relevant if warm line / hot line is to be configured:) The destination for warm line or hot line is set in **User menu > Configuration > Keyset > Lines**:



In the local phone menu, the menu path is the same.

Administration via Local Phone

The configuration of a line via Local phone is only possible when the line key has been created via Web interface or DLS before.

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- Keyset Lines	
|--- Details For Keyset Line <xx>	
|--- Address	
|--- Ring on/off	
|--- Selection order	
|--- Hot/warm action	

3.11.3 Configure Keyset Operation

The following parameters provide general settings which are common for all keyset lines.

The **Rollover ring** setting will be used when, during an active call, an incoming call arrives on a different line. If "no ring" is selected, the incoming call will not initiate a ring. If "alert ring" is selected, a 3 seconds burst of the configured ring tone is activated on an incoming call; "alert beep" selects a beep instead of a ring tone. "Standard ring tone" selects the default ringer.

LED on registration determines whether the line LEDs will be lit for a few seconds if they have been registered successfully with the SIP server on phone startup.

The **Originating line preference** parameter determines which line will be used when the user goes off-hook or starts on-hook dialing.

> ***INFO:*** When a terminating call exists, the terminating line preference takes priority over originating line preference.

The following preferences can be configured:

- "idle line": An idle line is selected. The selection is based on the Selection order parameter assigned to each line (see *Line Key Configuration*).
- "primary": The designated Primary Line/Main DN is always selected for originating calls.
- "last": The line selected for originating calls is the line that has been used for the last call (originating or terminating).
- "none": The user manually selects a line by pressing its line key before going off-hook or by pressing the speaker key, to originate a call.

Manual line selection overrides automatic line preferences.

The **Terminating line preference** parameter decides which terminating line, i. e. line with an incoming call, is selected when the user goes off-hook.

The following preferences can be configured:

- "ringing line": The line in the alerting or audible ringing state is automatically selected when the user goes off-hook. In the case of multiple lines alerting or ringing, the lines are selected on the one that has been alerting the longest.
- "ringing PLP": The line in the alerting or audible ringing state is automatically selected when the user goes off-hook. However, if the prime line is alerting, it is given priority.
- "incoming": The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected.
- "incoming PLP": The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected. However, if the prime line is alerting, it is given priority.
- "none": To answer a call, the user manually selects a line by pressing its line key be-fore going off-hook, or by pressing the speaker key.

Manual line selection overrides automatic line preferences.

Line action mode determines the consequence for an established connection when the line key is pressed. If "hold" is selected, the call currently active is set to hold as soon as the line key is activated. The user has two options: 1) to reconnect to the remote phone by pressing the line key that corresponds to that call, or 2) to initiate another call from the newly selected line. If "release" is selected, the previously established call is ended.

If **Show Focus** is checked, the LED of a line key flutters when the line is in use. If it is not checked, the line key is lit steady when it is in use.

The **Reservation timer** sets the period after which the reservation of a line is canceled. A line is automatically reserved for the keyset whenever the user has selected a line for an outgoing call and hears a dial tone. The reservation of a line is accomplished by the OpenScape Voice server, which notifies all the endpoints sharing this line. If set to 0, the reservation timer is deactivated.

Forward indication activates or deactivates the indication of station forwarding, i. e. the forwarding function of OpenScape Voice. If **Forward indication** is activated and station forwarding is active for the corresponding line, the LED of the line key blinks.

Preselect mode determines the phone's behavior when a call is active, and another call is ringing. If the parameter is set to "Single button", the user can accept the call a single press on the line key. If it is set to "Preselection", the user must first press the line key to select it and then press it a second time to accept the call. In both cases, the options for a ringing call are presented to the user: "Accept", "Reject", "Deflect".

Preselect timer is relevant if **Preselect mode** is set to "Preselection". The parameter sets the timeout in seconds for the second key press that is required to accept the call. After the timeout has expired, the call is no longer available.

When **Bridging enabled** is activated, the user may join into an existing call on a shared line by pressing the corresponding line key. On key press, OpenScape Voice builds a server based conference from the existing call parties and the user. If the call has already been in a server based conference, the user is added to this conference.

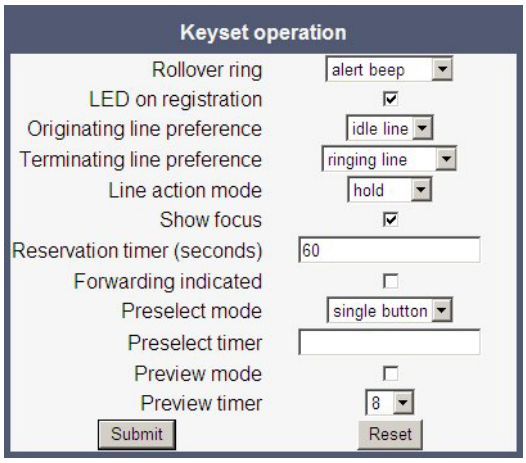
INFO: When bridging shall be used, it is highly recommended to configure the phone for a system based conference (see *System-Based Conference*). This enables adding more users to a system based conference that has been initiated by bridging.

Data required

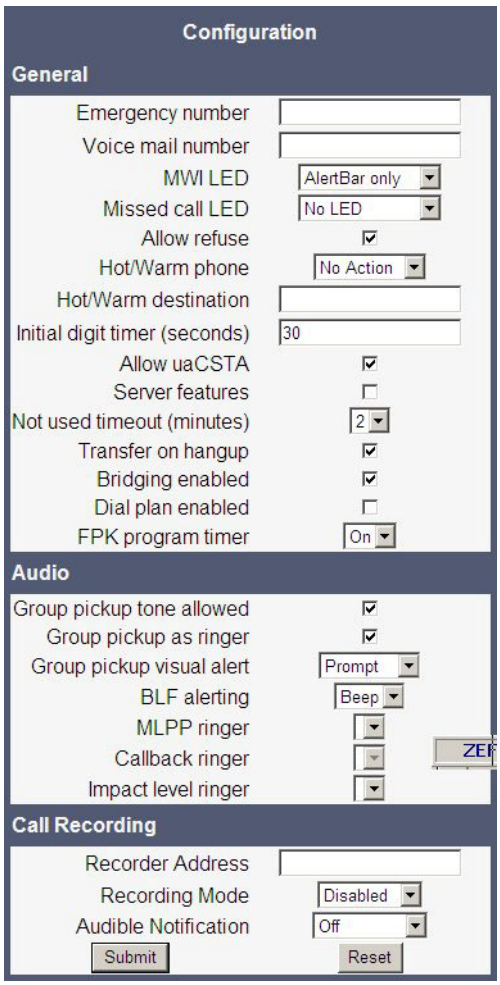
- **Rollover ring**: Determines if a ring tone will signal an incoming call while a call is active.
  Value range: "Standard ring", "No ring", "Alert beep", "Alert ring"
  Default: "Alert beep"
  LED on registration: Determines if line LEDs will signal SIP registration.
  Value range: "Yes", "No"
  Default: "Yes"
  Originating line preference: Selects the line to be used for outgoing calls.
  Value range: "Idle line", "Primary", "Last", "None"
  Default: "Idle line"
  Terminating line preference: Determines which line with an incoming call shall be selected for answering.
  Value range: "Ringing line", "Incoming", "Incoming PLP", "Ringing PLP", "None"
  Default: "Idle line"
  Line action mode: Determines the consequence for an established connection when the line key is pressed.
  Value range: "Hold", "Release"
  Default: "Hold"
  Show focus: Determines whether the line key LED blinks or is steady when it is in use.
  Value range: "Yes", "No"
  Default: "Yes"
  Reservation timer: Sets the period in seconds after which a line reservation is cancelled. If set to 0, the reservation timer is deactivated.
  Default: 60
  Forward indication: Activates or deactivates the indication of station forwarding.
  Value range: "Yes", "No"
  Default: "No"
  Preselect mode: Determines whether an incoming call is accepted by a single press on the corresponding line key or a double press is needed.
  Value range: "Single button", "Preselection"
  Default: "Single button"
  Preselect timer: Sets the timeout in seconds for accepting an incoming call.
  Bridging enabled : When set to "Yes", the user is allowed to join a call on a shared line. For this purpose, a server based conference is established.

Administration via WBM

System > Features > Keyset Operation



System > Features > Configuration



Administration via Local Phone

└--- Admin	
|--- System	
|--- Features	
|--- Keyset operation	
|--- Rollover ring	
|--- LED on registration	
|--- Originating line preference	
|--- Terminating line preference	
|--- Line action mode	
|--- Show focus	
|--- Reservation timer	
|--- Forward indicated	
|--- Preselect mode	
|--- Preselect timer	

Administration via Local Phone

└--- Admin	
|--- System	
|--- Features	
Configuration	
|--- General	
|--- Bridging enabled	

3.11.4 Line Preview

This key enables the preview mode, which allows the user to preview a line before using it.

When preview mode is active, the line keys behave similar to when the keyset configuration is set to preselection for line keys (see *Configure Keyset Operation*). On pressing the line key (not DSS key!), the call activity on the corresponding line is shown. Unlike with a preselected line, there will be no change to the phone's current line connections. The LED indicates whether line preview is active or not.

The information shown to the user depends on the ring/alert configuration for the line in question. If the line is configured to alert only, the preview will only show the state of the call, not the identity of the calling party. If the line is configured to ring, the identity of the calling party will be revealed.

The preview mode can be configured as temporary or as permanent. If **System > Features > Keyset operation > Preview mode** is disabled, preview mode will end when the user uses the previewed line, or a new call is started in any other way, or if the focus is changed away from call view. If the parameter is enabled, preview mode remains active until the user cancels it by pressing the key again.

The **Preview timer** parameter determines the time span during which the line preview will remain on the screen.

The Bridging priority parameter affects the behavior of the line key (see *Preview and Preselection*). Precondition: Bridging is enabled (see *Configure Keyset Operation*)

Administration via WBM

System > Features > Program keys > Preview

3.11.4.1 Preview and Preselection

Precondition: Bridging is enabled

Action	**Preselect mode**		**Preview mode**		**Bridging priority**		**Result**
	Single button	Pre-selec-tion	On (Lock Prev.)	Off (Temp Prev.)	Preview over-rides bridging	Bridg-ing over-rides preview	
Preview key is not pressed (LED off), only the Line key is pressed once or twice							
Press busy second. line key 1x	-	yes	n.rel.	n.rel.	n.rel.	n.rel.	Line status is dis-played (Preselect timer)
Press busy second. line key 2x while line-view is dis-played	-	yes	n.rel.	n.rel.	n.rel.	n.rel.	1st press: line sta-tus 2nd press: bridge (conference)
Press busy second. line key 1x	yes	-	n.rel.	n.rel.	n.rel.	n.rel.	Bridge (confer-ence)
Preview key is pressed first (LED on) and the Line key is pressed once or twice							
Press busy second. line key 1x	n.rel.	n.rel.	-	yes	-	yes	Bridge (confer-ence) Preview LED -> off

Press busy second. line key 1x	n.rel.	n.rel.	yes	-	-	yes	Bridge (conference) Preview LED remains on
Press busy second. line key 1x	n.rel.	n.rel.	-	yes	yes	-	Line status is displayed (Preview timer) Preview LED -> off
Press busy second. line key 1x	n.rel.	n.rel.	yes	-	yes	-	Line status is displayed (Preview timer) Preview LED remains on
Press busy second. line key 2x while line-view is displayed	n.rel.	n.rel.	-	yes	yes	-	1st press: line status 2nd press: bridge (conference) Preview LED -> off
Press busy second. line key 2x while line-view is displayed	n.rel.	n.rel.	yes	-	yes	-	1st press: line status 2nd press: bridge (conference) Preview LED remains on

In case the Preview key is not pressed, only the Preselection mode configuration is relevant:

- if Preselection is selected then the line status is displayed after 1st line press
- if Single button is selected then bridging is invoked (if line busy, bridging enabled)

In case the Preview key is pressed first and then the line key, the Preselection mode configuration is not relevant.

- if Preview mode is activated then the Preview key LED remains on (preview mode must be deactivated manually by pressing the Preview key again).
- if Preview mode is deactivated then the Preview key LED is turned off after preview timer expiry
  - if Bridging priority= Bridging overrides preview then pressing the busy line key invokes bridging
  - if Bridging priority= Preview overrides bridging then pressing the line key displays the line status, however pressing the line key twice bridging will be invoked.

3.11.5 Immediate Ring

Enables or disables the preset delay for all line keys. This feature only applies to keyset lines.

Use the **Key label <key number>** field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to *How to Configure Free Programmable Keys (FPKs)*.

Administration via WBM

System > Features > Program keys > Immediate ring

3.11.6 Direct Station Select (DSS)

INFO: This feature requires OpenScape Voice.

INFO: This feature can be enabled or disabled under System > Features > Feature access (see *Feature Access*).

A DSS key is a special variant of a line key. It enables a direct connection to a target phone, allowing the user to pick up or forward a call alerting the DSS target and make/complete a call to the DSS target.

3.11.6.1 General DSS Settings

These parameters define the behavior of all DSS keys.

INFO: Generally, it is advisable to restrict the user's possibilities to modify line keys, including DSS keys. This can be achieved solely by the DLS. For further instructions, see the *DLS Administration Guide*

If the user picks up an incoming call for the DSS target by pressing the associated DSS key, the call is forwarded to the user's primary line. Thereafter, the user's phone rings, and the user can accept the call.

> ***INFO:*** To enable the immediate answering of a call via the DSS key, **Allow auto-answer** in the **User** menu must be activated. The complete path on the WBM is: **User Pages > Configuration > Incoming calls > CTI calls > Allow auto-answer**.

The value of **Call pickup detect timer (seconds)** determines the time interval in which the deflected call is expected at the primary line. When the call arrives within this interval, it is given special priority and handling. If a second call arrives on the primary line during this interval, it will be rejected. If a second call arrives outside the interval, it will be treated just like any other incoming call. The default is 3.

If **Deflecting call enabled** is checked, the user can forward an alerting call to the DSS target by pressing the DSS key. The default is "No".

> ***INFO:*** This parameter is configured under System > Features > Feature access (see *Feature Access*).

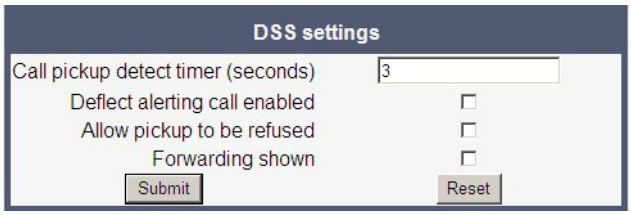
If **Allow pickup to be refused** is checked, the user is enabled to reject a call alerting on the line associated with the DSS key. The default is "No".

> ***INFO:*** This parameter is configured under System > Features > Feature access (see *Feature Access*).

The DSS key can be configured to indicate the call forwarding state of the number represented by the DSS key. This feature is activated when **Forwarding shown** is enabled.

Administration via WBM

System > Features > DSS Settings



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	

|--- DSS operation	
|--- Deflect to DSS	
|--- Refuse DSS pickup	
|--- Forwarding shown	

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- DSS Pickup timer	

3.11.6.2 Settings for a DSS key

The **Key label <n>** parameter provides the DSS key with a label that is displayed on the graphic display on OpenScape Desk Phones. The label is also user configurable.

Address contains the call number of the line associated with the DSS key.

The **Realm** parameter stores the SIP Realm of the line associated with the DSS key.

User Identifier gives the SIP user ID of the line associated with the DSS key.

Password provides the password corresponding to the SIP user ID.

The **Outgoing calls** parameter determines the behavior of a call over the DSS line at the target phone. If set to "Direct", any forwarding and Do not Disturb settings on the target phone will be overridden, so that a call will always alert. If set to Line type is set to "Normal", this is not the case, and the call will be treated like a regular call.

Action on calls defines the handling of an active call when pressing the DSS key. If set to "Consult", the user has an option to start a consultation with the DSS target. If set to "Transfer", the user can only transfer the call to the DSS target. If "No action" is selected, pressing the DSS key will have no effect.

When **Allow in Overview** is set to "Yes", the line corresponding to the DSS key will be visible in the line overview on the phone's display.

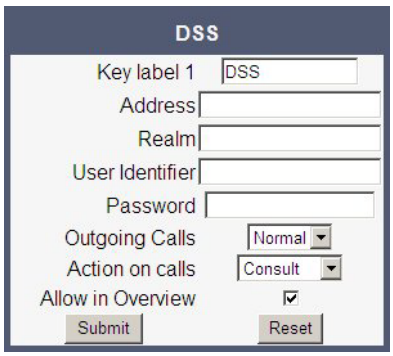
Data required

- **Key label <key number>**: Label to be displayed on the display.
  Default: "DSS"
- **Address**: SIP Address of Record of the destination that is assigned to the DSS key.
- **Realm**: SIP Realm of the DSS destination.

- **User ID**: SIP user ID of the DSS destination.
- **Password**: Password corresponding to the SIP user ID.
- **Outgoing calls**: Determines whether forwarding and DND at the target phone will be overridden on a DSS call.
  Value range: "Normal", "Direct"
  Default: "Normal"
- **Action on calls**: Handling of an active call when pressing the DSS key. "Consult": the user can start a consultation with the DSS target; "Transfer": the user can transfer the call to the DSS target.
  Value range: "Consult", "Transfer", "No action"
  Default: "Consult"
- **Allow in Overview**: Determines whether the line appears in the phone's line overview.
  Value range: "Yes", "No"
  Default: "Yes"

Administration via WBM

System > Features > Program keys > DSS



3.12 Dialing

3.12.1 Canonical Dialing Configuration

Call numbers taken from a directory application, LDAP for instance, are mostly expressed in canonical format. Moreover, call numbers entered into the local phone book are automatically converted and stored in canonical format, thereby adding "+", **Local country code, Local national code**, and **Local enterprise number** as prefixes. If, for instance, the user enters the extension "1234", the local country code is "49", the local national code is "89", and the local enterprise number is "722", the resulting number in canonical format is "+49897221234".

For generating an appropriate dial string, a conversion from canonical format to a different format may be required. The following parameters determine the local settings of the phone, like **Local country code** or **Local national code**, and define rules for converting from canonical format to the format required by the PBX.

> ***INFO:*** To enable the number conversion, all parameters not marked as optional must be provided, and the canonical dial lookup settings must be configured (see *Canonical Dial Lookup*).

Data required

- **Local country code**: E.164 Country code, e.g. "49" for Germany, "44" for United Kingdom. Maximum length: 5
- **National prefix digit**: Prefix for national connections, e.g. "0" in Germany and United Kingdom. Maximum length: 5
- **Local national code**: Local area code or city code, e.g. "89" for Munich, "20" for London. Maximum length: 6
- **Minimal local number length**: Minimum number of digits in a local PSTN number, e.g. 3335333 = 7 digits.
- **Local enterprise number**: Number of the company/PBX wherein the phone is residing. Maximum length: 10 (Optional)
- **PSTN access code**: Access code used for dialing out from a PBX to a PSTN. Maximum length: 10 (Optional)
- **International access code**: International prefix used to dial to another country, e.g. "00" in Germany and United Kingdom. Maximum length: 5
- **Operator codes**: List of extension numbers for a connection to the operator. The numbers entered here are not converted to canonical format. Maximum length: 50 (Optional)
- Emergency number: List of emergency numbers to be used for the phone. If there are more than one numbers, they must be separated by commas. The numbers entered here are not converted to canonical format. Maximum length: 50 (Optional) These emergency numbers can also be dialed when the phone is locked, in line with the emergency number configured in Features > Configuration (see *Emergency and Voice Mail*).
- **Initial extension digits / Initial digits**: List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly. If, for instance, the extensions 3000-5999 are configured in OpenScape Voice, each number will start with 3, 4, or 5. Therefore, the digits to be entered are 3, 4, 5.

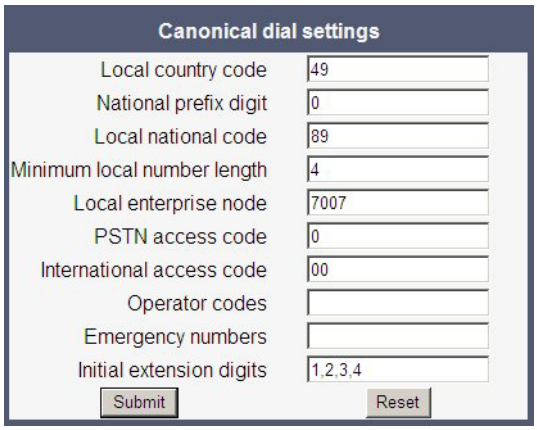
- **Internal numbers**

  INFO: To enable the phone to discern internal numbers from external numbers, it is crucial that a canonical lookup table is provided (*Canonical Dial Lookup*).

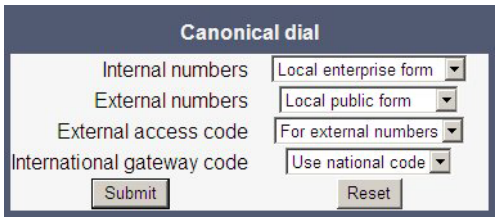
  – **Local enterprise form**: Default value. Any extension number is dialed in its simplest form. For an extension on the local enterprise node, the node ID is omitted. If the extension is on a different enterprise node, then the appropriate node ID is prefixed to the extension number. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
  – **Always add node**: Numbers that correspond to an enterprise node extension are always prefixed with the node ID, even those on the local node. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
  – **Use external numbers**: All numbers are dialed using the external number form.
- **External numbers**
  – **Local public form**: Default value. All external numbers are dialed in their simplest form. Thus a number in the local public network region does not have the region code prefix. Numbers in the same country but not in the local region are dialed as national numbers. Numbers for a different country are dialed using the international format.
  – **National public form**: All numbers within the current country are dialed as national numbers, thus even local numbers will have a region code prefix (as dialing from a mobile). Numbers for a different country are dialed using the international format.
  – **International form**: All numbers are dialed using their full international number format.
- **External access code**
  – **Not required**: The access code to allow a public network number to be dialed is not required.
  – **For external numbers**: Default value. All public network numbers will be prefixed with the access code that allows a number a call to be routed outside the enterprise network. However, international numbers that use the + prefix will not be given access code.
- **International gateway code**:
  – **Use national code**: Default value. All international formatted numbers will be dialed explicitly by using the access code for the international gateway to replace the "+" prefix.
  – **Leave as +**: All international formatted numbers will be prefixed with "+".

Administration via WBM

Local functions > Locality > Canonical dial settings



Local functions > Locality > Canonical dial



Administration via Local Phone

|--- Admin	
|--- Local Functions	
|--- Locality	
|--- Canonical settings	
|--- Local country code	
|--- National prefix digit	
|--- Local national code	
|--- Minimum local number length	
|--- Local enterprise node	
|--- PSTN access code	
|--- International code	
|--- Operator code	
|--- Emergency number	
|--- Initial digits	

|--- Admin	
|--- Local Functions	
|--- Locality	
|--- Canonical dial	
|--- Internal numbers	
|--- External numbers	
|--- External access code	
|--- International gateway	

3.12.2 Canonical Dial Lookup

The parameters given here are important for establishing outgoing calls and for recognizing incoming calls.

In the local phonebook, and, mostly, in LDAP directories, numbers are stored in canonical format. In order to generate an appropriate dial string according to the settings in Internal numbers and External numbers (*Canonical Dialing Configuration*), internal numbers must be discerned from external numbers. The canonical lookup table provides patterns which allow for operation.

Furthermore, these patterns enable the phone to identify callers from different local or international telephone networks by looking up the caller's number in the phone book. As incoming numbers are not always in canonical format, their composition must be analyzed first. For this purpose, an incoming number is matched against one or more patterns consisting of country codes, national codes, and enterprise nodes. Then, the result of this operation is matched against the entries in the local phone book.

INFO: To make sure that canonical dial lookup works properly, at least the following parameters of the phone must be provided:

- Local country code (*Canonical Dialing Configuration*)
- Local area code (*Canonical Dialing Configuration*)
- Local enterprise code (*Canonical Dialing Configuration*)

Up to 5 patterns can be defined. The Local code 1 ... 5 parameters define up to 5 different local enterprise nodes, whilst International code 1... 5 define up to 5 international codes, that is, fully qualified E.164 call numbers for use in a PSTN.

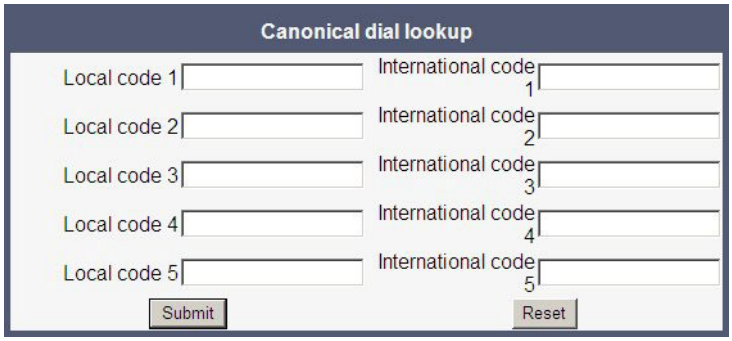
Data required

- **Local code 1 ... 5**: Local enterprise code for the node/PBX the phone is connected to. Example: "722" for Siemens Munich.

- **International code 1 ... 5**: Sequence of "+", local country code, local area code, and local enterprise node corresponding to to one or more phone book entries. Example: "+4989722" for Siemens Munich.

Administration via WBM

Locality > Canonical dial lookup



Administration via Local Phone

|--- Admin
|--- Local Functions
|--- Locality
|--- Canonical Lookup
|--- Local code 1
|--- International 1
|--- Local code 2
|--- International 2
|--- Local code 3
|--- International 3
|--- Local code 4
|--- International 4
|--- Local code 5
|--- International 5

3.12.3 Dial Plan

OpenScape Desk Phones may optionally use a dial plan residing on the phone. By means of the dial plan, the phone can infer from the digits entered by the user that a complete call number has been entered, or that a particular prefix has been entered. Thus, the dialing process can start without the need to confirm after the last digit has been entered, without delay or with a configurable delay. The

standard timer, which is found on the WBM under **User menu > Configuration > Outgoing calls > Autodial delay (seconds)**, is overridden if a dial plan rule is matched.

A dial plan consists of rules defining patterns, timeouts and actions to be performed when a pattern is matched and/or a timeout has expired. The phone can store one dial plan, which can contain up to 48 different rules.

It is very important that the phone's dial plan does not interfere with the dial plan in the SIP server, PBX, or public network.

The dial plan can be created and uploaded to the phone using the DLS (please refer to the OpenScape Deployment Service Administration Manual). The DLS can also export and import dial plans in .csv format. For details about the composition of a dial plan, please refer to *Example Dial Plan*.

The current dial plan, along with its status (enabled/disabled) and error status can be displayed on the WBM via **Diagnostics > Fault trace configuration > Download dial plan file**.

The **Dial plan ID** and the **Dial plan status** is displayed in the local menu.

To make use of the dial plan facility, the following requirements must be met:

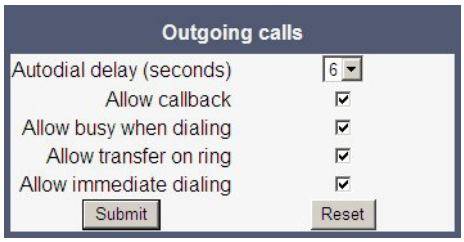
- A correct dial plan is loaded to the phone.
- In the user menu, **Allow immediate dialing** is enabled.

> ***INFO:*** This condition is only necessary for on-hook dialing, but not for off-hook dialing.

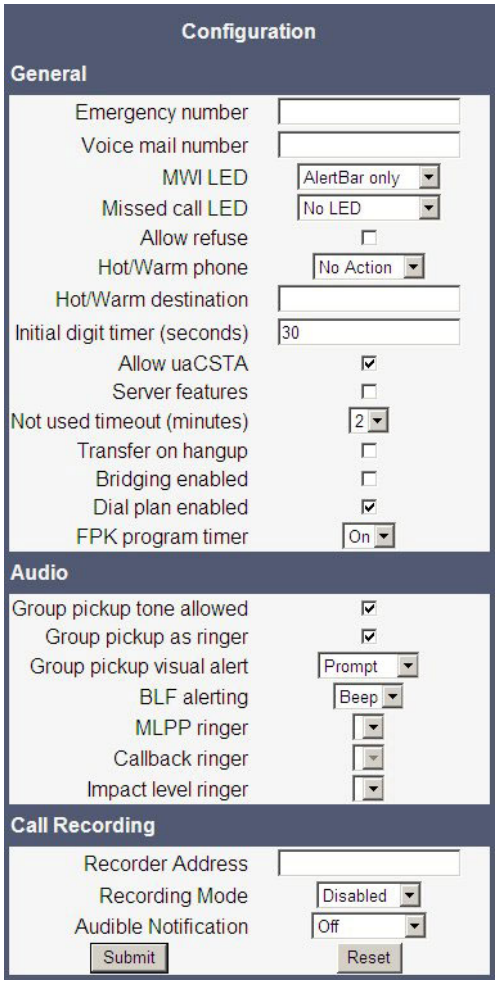
- **Dial plan enabled** is checked.

Administration via WBM

User menu > Configuration > Outgoing calls > Allow immediate dialing



System > Features > Configuration > Dial plan enabled



Administration via Local Phone

|--- User
|--- Configuration
|--- Outgoing calls
|--- Immediate dialing

|--- Admin
|--- System
|--- Features
|--- Configuration
|--- General
|--- Dial plan

└--- Admin	
|--- General Information	
|--- Dial plan ID	
|--- Dial plan status	

3.13 Distinctive Ringing

The SIP server may provide information indicating a specific type of call within an incoming call. The phone can use this information to choose a ring tone according to the call type.

The relevant information is carried as a string in the SIP Alert-Info header. This string is configured in the OpenScape Voice system; please refer to the relevant OpenScape Voice documentation. When the string sent via Alert-Info matches the string specified in the Name parameter, the corresponding ringer is triggered. For instance, the OpenScape Voice system may send the string `Bellcore-dr1` to indicate that a call is from within the same business group, and the **Name** parameter is set to "Bellcore-dr1". To select a specific ring tone for calls from the same business group, the other parameters corresponding to that **Name** must be set accordingly.

The **Ringer sound** parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.

Pattern Melody selects the melody pattern that will be used if **Ringer sound** is set to "Pattern".

Pattern sequence determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:

- "1": 1 sec ON, 4 sec OFF
- "2": 1 sec ON, 2 sec OFF
- "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF

The **Duration** parameter determines how long the phone will ring on an incoming call. The range is 0-300 sec.

With the **Audible** parameter, the ringer can be muted. In this case, an incoming call will be indicated only visually.

Special Ringers can be configured for the following call types:

- Internal
- External
- Recall

- Emergency

> ***INFO:*** To make the special ringers available and configurable to the user, the administrator needs to map the call types to specific ringers via the **Ringer setting** mapping table in **Admin > Ringer setting > Distinctive**. Each call type can be mapped to a specific Ringer Sound, Pattern Melody and Pattern Sequence.

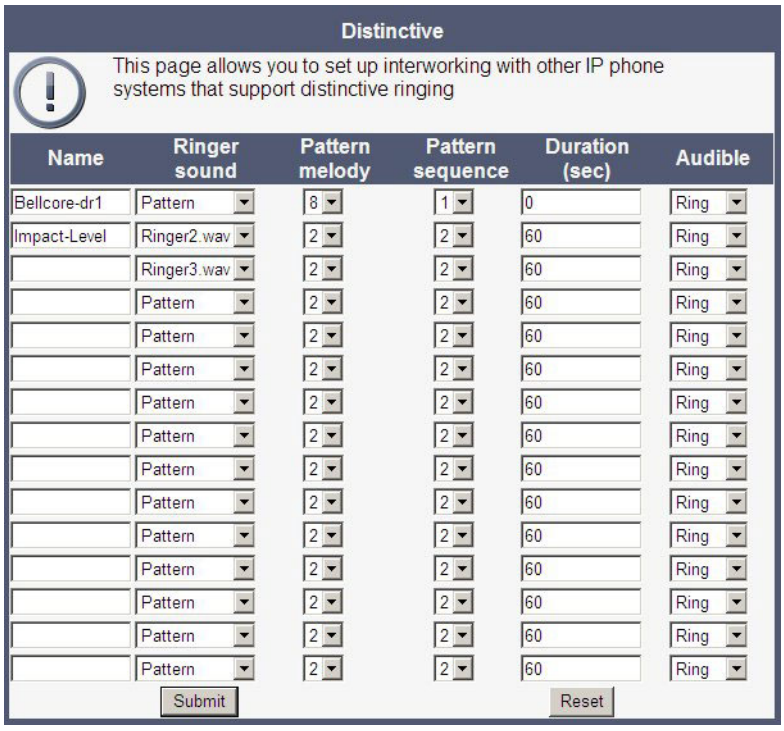
The OSCAR client specification defines the following abstract names for use between SEN equipment:

- "<Bellcore-dr1>" - normal (internal) alerting or ring-back;
- "<Bellcore-dr2>" - external alerting or ring-back;
- "<Bellcore-dr3>" - recall alerting or ring-back, (e.g., following transfer);
- "<alert-internal>" - normal (internal) alerting or ring-back;
- "<alert-external>" - external alerting or ring-back;
- "<alert-recall>" - recall alerting or ring-back, (e.g., following transfer);
- "<alert-emergency>" - emergency alerting or ring-back.

Once made available (by the administrator) to the user, the Special Ringers for the call types listed can be selected and configured via the User menu as shown in *Special Ringers*.

Administration via WBM

Ringer Setting > Distinctive



Administration via Local Phone

|--- Admin	
|--- Ringer setting	
|--- Distinctive	
|--- <1 .... 15>	
|--- Name	
|--- Ringer sound	
|--- Pattern melody	
|--- Pattern sequence	
|--- Duration	
|--- Audible	

3.13.1 Special Ringers

Special Ringers can be configured via the **User** menu for the following call types:

- Internal
- External
- Recall
- Emergency

Administration via WBM (User menu)

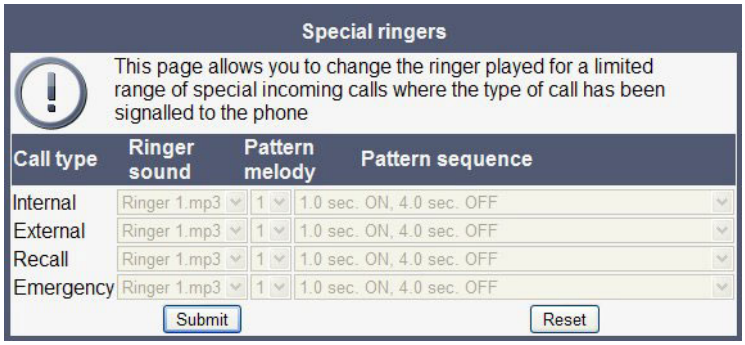
User menu > Audio > Special Ringers

The **Special Ringers** dialog allows the user to change the ring tones for the special call types listed below, provided that the call type is signaled to the phone.

> ***INFO:*** To make the special ringers available and configurable to the user, the administrator needs to map the call types to specific ringers via the **Ringer setting** mapping table in **Admin > Ringer setting > Distinctive**. Each call type can be mapped to a specific Ringer Sound, Pattern Melody and Pattern Sequence.

Special Ringer Call Types

- Internal
- External
- Recall
- Emergency



Administration via Local Phone

|--- User	
|--- Audio	
|--- Special Ringers	
|--- Internal	
|--- External	
|--- Recall	
|--- Emergency	

For each call type, the following parameters can be configured:

The **Ringer sound** parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.

Pattern Melody selects the melody pattern that will be used if Ringer sound is set to "Pattern".

Pattern sequence determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:

- "1": 1 sec ON, 4 sec OFF
- "2": 1 sec ON, 2 sec OFF
- "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF

3.14 Mobility

The Mobility feature requires the OpenScape Deployment Service (DLS). If the phone is mobility enabled by the DLS, a mobile user can log on to the phone and thereby have his/her own user settings transferred to the phone. These user data are stored in the DLS database and include, for instance, SIP registration settings, dialing properties, key layouts, as well as the user's phonebook.

If the mobile user changes some settings, the changed data is sent to the DLS server. This ensures that the user profile is updated if necessary.

If **Unauthorized logoff trap** is set to "Yes", a message is sent to the SNMP server if an unauthorized attempt is made to log off the mobile user.

Logoff trap delay defines the time span in seconds between the unauthorized logoff attempt and the trap message to the SNMP server.

Timer med priority determines the time span in seconds between a change of user data in the phone and the transfer of the changes to the DLS server.

The **Mobility feature** parameter indicates whether the mobility feature is enabled by the DLS or not.

Data required

- **Unauthorized logoff trap**: An SNMP trap is sent on an unauthorized logoff attempt.
  Value range: "Yes", "No"
  Default: "No"
- **Logoff trap delay**: Time span in seconds between the unauthorized logoff attempt and the SNMP trap.
  Default: 300
- **Timer med priority**: Time span in seconds between a data change in the phone and its transfer to the DLS server.
  Default: 60
- **Mobility feature**: Indicates whether the mobility feature is enabled.
- **Managed profile**
- **Error count local**
- **Error count remote**

Administration via WBM

Administration via Local Phone

└--- Admin	
|--- Mobility	
|--- Unauthorized Logoff Trap	
|--- Logoff Trap Delay	
|--- Timer Medium Priority	
|--- Mobility Feature	

|--- Managed Profile	
|--- Error Count Local	
|--- Error Count Remote	

3.15 Transferring Phone Software, Application and Media Files

New software images, hold music, LDAP templates, and ring tones can be uploaded to the phone via DLS (Deployment Service) or WBM (Web Based Management).

INFO: For all user data, which includes files as well as phonebook content, the following amounts of storage place are available:

- OpenScape Desk Phone IP 35G: 4 MB
- OpenScape Desk Phone IP 55G: 8 MB

3.15.1 FTP/HTTPS Server

FTP Server Requirements

There are no specific requirements regarding the FTP server for transferring files to the OpenScape Desk Phone. Any FTP server providing standard functionality will do.

3.15.2 Common FTP/HTTPS Settings

For each one of the various file types, e.g. phone software, hold music, and picture clips, specific FTP/HTTPS access data can be defined. If some or all file types have the parameters **Download method**, **Server address**, **Server port**, **Account**, **User name**, **FTP path**, and **HTTPS base URL** in common, they can be specified here. These settings will be used for a specific file type if its **Use defaults** parameter is set to "Yes".

INFO: If Use defaults is activated for a specific file type, any specific settings for this file type are overridden by the defaults.

Additional log messages are issued for the following scenarios:

- Update has been allowed due to override flag being set
- Whole part number is not recognised
- Block 4 of part number is not recognised

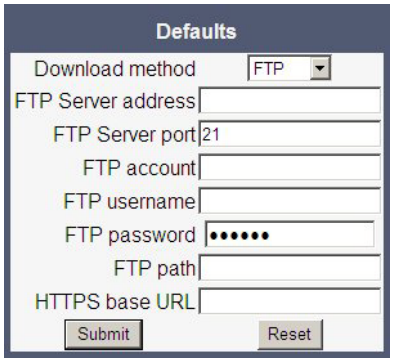
- Downloaded software does not have a hardware level included

Data required

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP server in use.
- **Server port**: Port number of the FTP server in use. For HTTPS, port 443 is assumed, unless a different port is specified in the HTTPS base URL.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use. If no port number is specified here, port 443 is used. Only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Defaults



Administration via Local Phone

└--- Admin	
|--- File Transfer	
|--- Defaults	
|--- Download method	
|--- Server	
|--- Port	
|--- Account	
|--- Username	

|--- Password	
|--- FTP path	
|--- HTTPS base URL	

3.15.3 Phone Software

The firmware for the phone can be updated by downloading a new software file to the phone.

If an incorrect software image is being attempted to be loaded onto the phone, the phone will reject the request and return to normal operation without reboot. As part of this security mechanism, new software binds are identified by a "Supported Hardware Level" information built into the header.

Prerequisite: The phone knows it’s own hardware level (from the part number and/or by a dynamical check of its HW level).

When a new software bind is downloaded to the phone, the following verifcation is performed:

1. 1. If new software bind has hardware level header included (in the bind header): Hardware level of new bind is compared with phone’s hardware level.
   - If compatible (or if Override is set): Proceed with update
   - If NOT compatible: Abandon update and return to original application
2. If new software bind does NOT have hardware level header included (in the bind header): Software version of new bind is compared with minimum known supported SW level.
   - If compatible (or if Override is set): Proceed with update
   - If NOT compatible: Abandon update and return to original application

INFO: Do not disconnect the phone from the LAN or power unit during software update. An active update process is indicated by blinking LEDs and/or in the display.

3.15.3.1 FTP/HTTPS Access Data

If the default FTP/HTTPS Access settings (see *Common FTP/HTTPS Settings*) are to be used, Use default must be set to "Yes", and only the Filename must be specified.

Data required (in every case)

- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No".
  Default: "No".

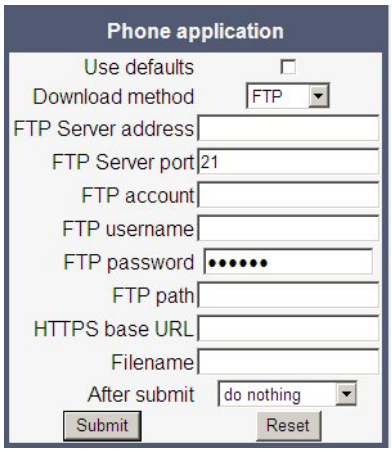
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base** URL: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Phone application



Administration via Local Phone

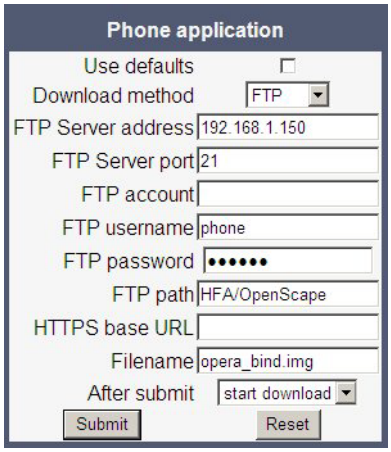
|--- Admin	
|--- File Transfer	
|--- Phone app	
|--- Details	
|--- Use default	
|--- Download method	
|--- Server	
|--- Port	
|--- Account	

|--- Username	
|--- Password	
|--- FTP path	
|--- HTTPS base URL	
|--- Filename	

3.15.3.2 Download/Update Phone Software

If applicable, phone software should be deployed using the DLS (OpenScape Deployment Service). Alternatively, the download can be triggered from the Web interface or from the Local phone menu. When the download has been successful, the phone will restart and boot up using the new software.

Start Download via WBM



In the **File transfer > Phone application** dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the **Admin** menu, set the focus to **Phone app**.

|--- Admin	
|--- File Transfer	
|--- Phone app	

Press the **>** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.15.4 Music on Hold

If enabled by the user, the Music on Hold (MoH) sound file is played when a call is put on hold.

> ***INFO:*** The file size for a Music on Hold file is limited to 1 MB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

The following formats for Music on Hold are supported:

- WAV format. The recommended specifications are:
  - Audio format: PCM
  - Bitrate: 16 kB/sec
  - Sampling rate: 8 kHz
  - Quantization level: 16 bit
- MIDI format
- MP3 format (on OpenScape Desk Phone IP 55G only): A bitrate of 48 kB/sec is recommended.

3.15.4.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see *Common FTP/HTTPS Settings*) are to be used, Use Default must be set to "Yes", and only the Filename must be specified.

Data required (in every case)

- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.

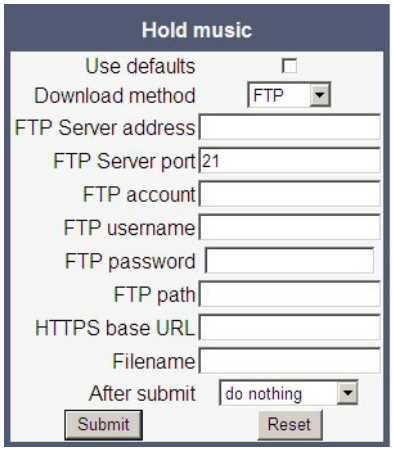
Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.

- **HTTPS base** URL: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Hold music



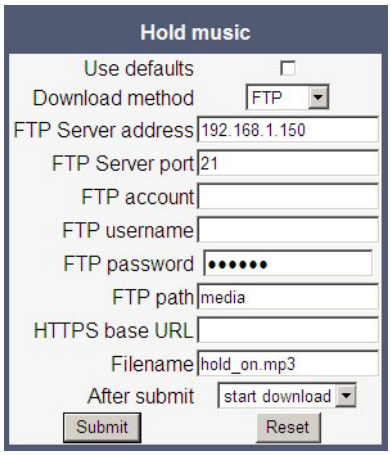
Administration via Local Phone

|--- Admin	
|--- File Transfer	
|--- Hold Music	
|--- Details	
|--- Use default	
|--- Download method	
|--- Server	
|--- Port	
|--- Account	
|--- Username	
|--- Password	
|--- FTP path	
|--- HTTPS base URL	
|--- Filename	

3.15.4.2 Download Music on Hold

If applicable, Music on Hold should be deployed using the DLS (OpenScape Deployment Service). Alternatively, the download can be triggered from the Web interface or from the Local phone menu.

Start Download via WBM



In the **File transfer > Hold music** dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **Hold Music**.

|--- Admin	
|--- File Transfer	
|--- Hold Music	

Press the **>** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.15.5 Ringer File

Custom ring tones can be uploaded to the phone.

> ***INFO:*** The file size for a ringer file is limited to 1 MB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone. This limitation is only enforced on WEBM, if a ringer file is downloaded via OpenStage Manager, this restriction does not apply.

The following file formats are supported:

- WAV format. The recommended specifications are:
  - Audio format: PCM
  - Bitrate: 16 kB/sec
  - Sampling rate: 8 kHz
- Quantization level: 16 bit

- MIDI format.
  MP3 format. The OpenScape Desk Phones (IP 55G only) are able to play MP3 files from 32 kbit/s up to 320 kbit/s. As the memory for user data is limited to 8 MB, a constant bitrate of 48 kbit/sec to 112 kbit/s and a length of max. 1 minute is recommended. Although the phone software can play stereo files, mono files are recommended, as the phone has only 1 loudspeaker. See the following table for estimated file size (mono files):

Length	64 kbit/s	80 kbit/s	96 kbit/s	112 kbit/s
0:15 min	0,12 MB	0,15 MB	0,18 MB	0,21 MB
0:30 min	0,23 MB	0,29 MB	0,35 MB	0,41 MB
0:45 min	0,35 MB	0,44 MB	0,53 MB	0,62 MB
1:00 min	0,47 MB	0,59 MB	0,70 MB	0,82 MB

3.15.5.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see *Common FTP/HTTPS Settings*) are to be used, Use default must be set to "Yes", and only the Filename must be specified.

Data required (in every case)

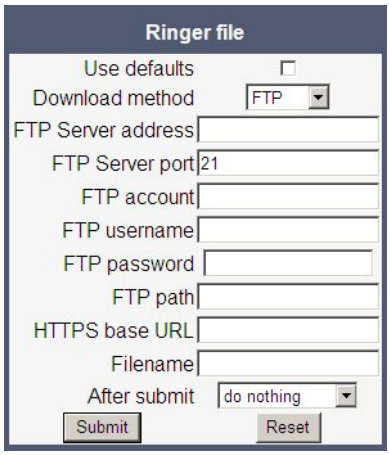
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
  Filename: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".

Administration via WBM

File transfer > Ringer file



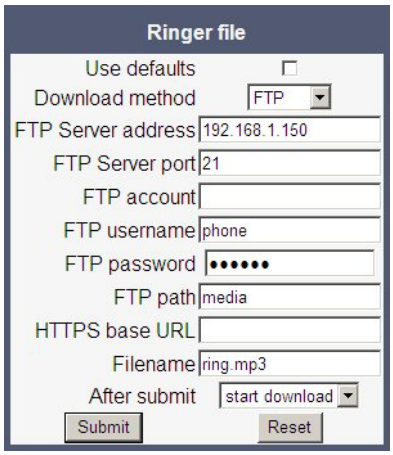
Administration via Local Phone

|--- Admin	
|--- File Transfer	
|--- Ringer	
|--- Details	
|--- Use default	
|--- Download method	
|--- Server	
|--- Port	
|--- Account	
|--- Username	
|--- Password	
|--- FTP path	
|--- HTTPS base URL	
|--- Filename	

3.15.5.2 Download Ringer File

If applicable, ring tone files should be deployed using the DLS (OpenScape Deployment Service). Alternatively, the download can be triggered from the Web interface or from the Local phone menu.

Start Download via WBM



In the **File transfer > Ringer** dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the **Admin** menu, set the focus to **Ringer**.

|--- Admin	
|--- File Transfer	
|--- Ringer	

Press the **>** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.15.6 Dongle Key

The HPT dongle key is a special file that contains a secret hash number which is required to connect the HPT tool to the phone. This testing tool is used exclusively by the service staff.

3.15.6.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see *Common FTP/HTTPS Settings*) are to be used, Use default must be set to „Yes“, and only the Filename must be specified.

Data required (in every case)

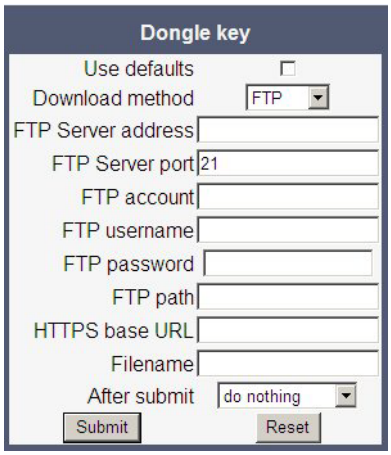
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: „Yes“, „No“
  Default: „No“
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: „FTP“, „HTTPS“
  Default: „FTP“
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if Download method is switched to „HTTPS“.

Administration via WBM

File transfer > Dongle key



Administration via Local Phone

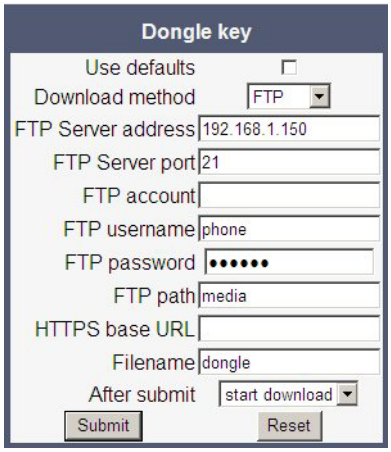
|--- Admin	
|--- File Transfer	
|--- Dongle key	
|--- Details	
|--- Use default	
|--- Download method	
|--- Server	
|--- Port	
|--- Account	
|--- Username	

|--- Password	
|--- FTP path	
|--- HTTPS base URL	
|--- Filename	

3.15.6.2 Download Dongle Key File

If applicable, dongle key files should be deployed using the DLS (OpenScape Deployment Service). Alternatively, the download can be triggered from the Web interface or from the Local phone menu.

Start Download via WBM



In the **File transfer > Dongle key** dialog, set **After submit** to „start download“ and press the **Submit** button.

Start Download via Local Phone

1. In the **Admin** menu, set the focus to **Dongle key**.

|--- Admin	
|--- File Transfer	
|--- Dongle key	

Press the **>** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.16 Speech

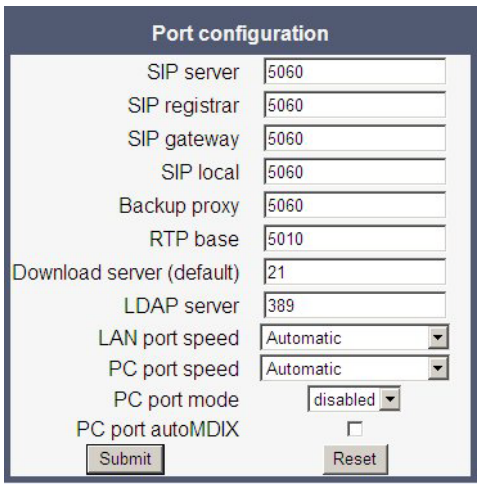
3.16.1 RTP Base Port

The port used for RTP is negotiated during the establishment of a SIP connection. The RTP base port number defines the starting point from which the phone will count up when negotiating. The default value is 5010.

The number of the port used for RTCP will be the RTP port number increased by 1.

Administration via WBM

Network > Port Configuration



Administration via Local Phone

|--- Admin	
|--- Network	
|--- Port Configuration	
|--- RTP base	

3.16.2 Codec Preferences

If **Silence suppression** is activated, the transmission of data packets is suppressed on no conversation, that is, if the user doesn't speak.

The OpenScape Desk Phone provides the codecs **G.711**, **G.722**, and **G.729**. When a SIP connection is established between two endpoints, the phones negotiate the codec to be used. The result of the negotiation is based on the general availability and ranking assigned to each codec. The administrator can allow or disallow a codec as well as assign a ranking number to it.

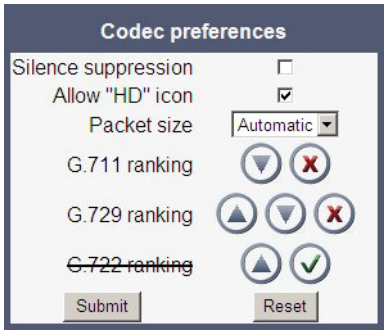
The **Packet size**, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10ms, 20ms, 30ms, 60ms or to automatic detection.

Data required

- **Silence suppression**: Suppression of data transmission on no conversation.
  Value range: "On", "Off"
  Default: "Off"
- **Allow "HD" icon**: If "On" an additional icon is shown when codec G.722 is used.
  Value range: "On", "Off"
  Default: "On"
- **Packet size**: Size of RTP packets in milliseconds.
  Value range: "10 ms", "20ms", "30ms", "60ms", "Automatic"
  Default: "Automatic"
- **G.711**: Parameters for the G. 711 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Choice 1"
- **G.729**: Parameters for the G. 729 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Choice 2"
- **G.722**: Parameters for the G. 722 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Disabled"

Administration via WBM

Speech > Codec preferences



Administration via Local Phone

|--- Admin	
|--- Speech	
|--- Codec Preferences	
|--- Silence suppression	
|--- Packet size	
|--- G.711	

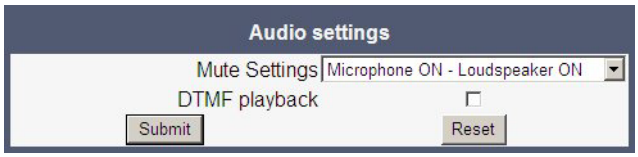
|--- G.729	
|--- G.722	
|--- Allow "HD" icon	

3.16.3 Audio Settings

The usage of microphone and speaker for speakerphone mode can be controlled by the administrator. Both microphone and loudspeaker can be switched on or off separately. By default, both microphone and loudspeaker are switched on.

Administration via WBM

Speech > Audio Settings



Administration via Local Phone

|--- Admin	
|--- Speech	
|--- Audio Settings	
|--- Disable microphone	
|--- Disable loudspeech	
|--- DTMF playback	

The **DTMF playback** feature aims at the capability to play DTMF digits received using RFC2833 coding (i.e. Rtp events) in the current active audio device (headset / loudspeaker / handset).

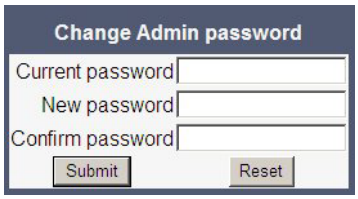
3.17 Password

The passwords for user and administrator can be set here. They have to be confirmed after entering. The factory setting for the administrator password is "123456"; it should be changed after the first login (see *Change Admin and User password*). The factory setting for the user password is "not set", i. e. empty.

Usable characters are 0-9 A-Z a-z .*#,?!'+-()@/:_

Administration via WBM

Security and Policies > Password > Change Admin password



Security and Policies > Password > Change User password

Administration via Local Phone

└--- Admin	
|--- Security & policies	
|--- Password	
|--- Change Admin password	
|--- Change User password	
|--- Confirmation	

3.18 Troubleshooting: Lost Password

If the administration and/or user password is lost, and there is no DLS available, new passwords must be provided. For this purpose, a factory reset is necessary. Take the following steps to initiate a factory reset:

1. Press the number keys 2-8-9 simultaneously. The Factory Reset menu opens.

   INFO: The Factory reset claw option needs to be enabled for this to work - see *Access Control*.

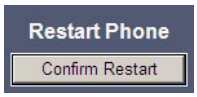
2. In the input field, enter the special password for factory reset: "124816".
3. Confirm by pressing **OK**.

3.19 Restart Phone

If necessary, the phone can be restarted from the administration menu.

Administration via WBM

Maintenance > Restart Phone



3.20 Factory Reset

This function resets all parameters to their factory settings. A special reset password is required for this operation: "124816".

Administration via WBM

Maintenance > Factory reset

Administration via Local Phone

└--- Admin	
|--- Maintenance	
|--- Factory reset	

3.21 SSH – Secure Shell Access

The phone's operating system can be accessed via SSH for special trouble-shooting tasks. Administration via DLS is also supported. Hereby, the administrator is enabled to use the built-in Linux commands. As soon as SSH access has been enabled using the WBM, the system can be accessed by the user "admin" for a specified time span. When this time span has expired, no connection is possible any more. The user "admin" has the following permissions:

- Log folder and files: read only
- User data folder and files: read/write access
- Opera deploy folders and files: read only
- Version folder: read/write access; version files: read only

INFO: It is not possible to logon as root via SSH.

When **Enable access** is enabled, and the parameters described underneath are specified, SSH access is activated. By default, SSH access is disabled.

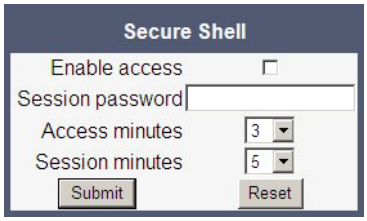
With the **Session password** parameter, a password for the "admin" user is created. This password is required. It will be valid for the time span specified in the parameters described underneath.

Access minutes defines the time span in minutes within which the SSH connection must be established. After it has expired, a logon via SSH is not possible. The possible values (as of V3) are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

Session minutes defines the maximum length in minutes for an SSH connection. After it has expired, the "admin" user is logged out. The possible values are 5, 10, 20, 30, 60.

Administration via WBM

Maintenance > Secure Shell



3.22 Display License Information

The license information for the OpenScape Desk Phone software currently loaded can be viewed via the local menu.

INFO: The license information can also be viewed by users who logged on using the User login if logging on as Admin is not permitted.

|--- Admin	
|--- Licence information	

3.23 Diagnostics

INFO: Some of the diagnostic tools and functions may reveal personal data of the user, such as caller lists. Thus, with regards to data privacy, it is recommended to inform the user when diagnostic functions are to be executed.

3.23.1 Display General Phone Information

General information about the status of the phone can be displayed if desired.

Displayed Data

- **MAC address**: Shows the phone's MAC address.

- **Software version**: Displays the version of the phone's firmware.
- **Last restart**: Shows date and time of the last reboot.
- **Backlight type**: Indicates whether the phone has a backlight, and, if applicable, the type of backlight.
  Value range: 0 (no backlight); 1 (cathode tube backlight); 2 (LED backlight)

Display on the WBM

General information

Display on the Local Phone

└--- Admin	
|--- General Information	
|--- MAC address	
|--- Software version	
|--- Last restart	
|--- Dial plan ID	
|--- Dial plan status	

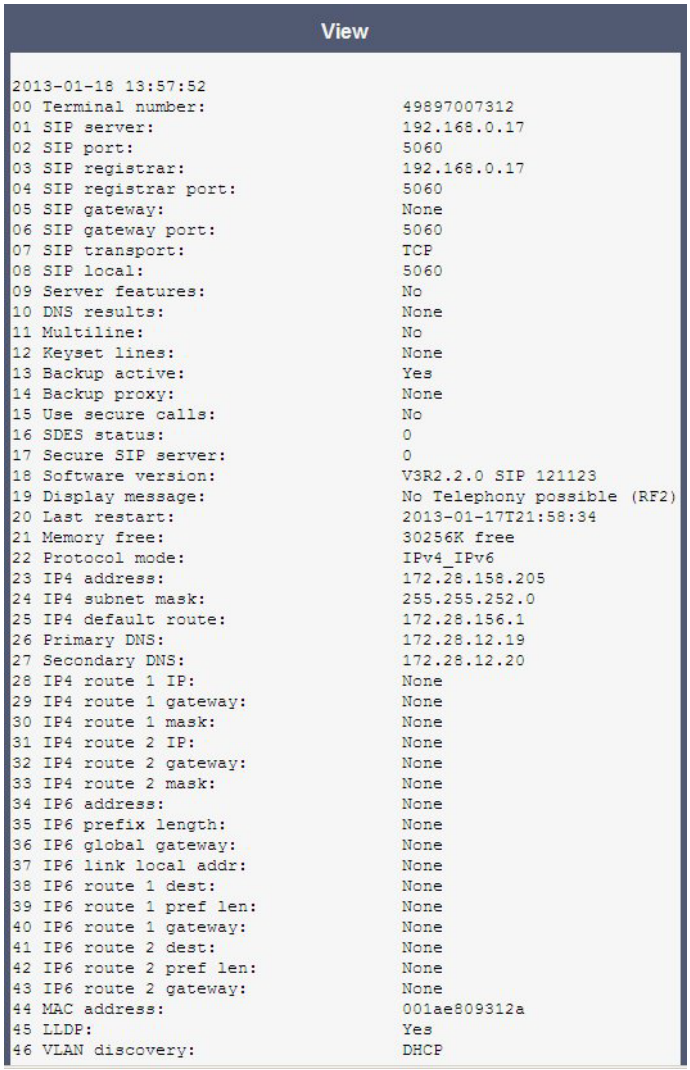
3.23.2 View Diagnostic Information

In addition to the general phone information (see *Display General Phone Information*), extended data can be viewed.

> ***INFO:*** The Diagnostic Information can also be viewed by the administrator on the local phone by selecting **Diagnostic information > View**.

Display on the WBM

Diagnostics > Diagnostic information > View



View

```
2013-01-18 13:57:52
00 Terminal number:                49897007312
01 SIP server:                     192.168.0.17
02 SIP port:                       5060
03 SIP registrar:                  192.168.0.17
04 SIP registrar port:             5060
05 SIP gateway:                    None
06 SIP gateway port:               5060
07 SIP transport:                  TCP
08 SIP local:                      5060
09 Server features:                No
10 DNS results:                    None
11 Multiline:                      No
12 Keyset lines:                   None
13 Backup active:                  Yes
14 Backup proxy:                   None
15 Use secure calls:               No
16 SDES status:                    0
17 Secure SIP server:              0
18 Software version:               V3R2.2.0 SIP 121123
19 Display message:                No Telephony possible (RF2)
20 Last restart:                   2013-01-17T21:58:34
21 Memory free:                    30256K free
22 Protocol mode:                  IPv4_IPv6
23 IP4 address:                    172.28.158.205
24 IP4 subnet mask:                255.255.252.0
25 IP4 default route:              172.28.156.1
26 Primary DNS:                    172.28.12.19
27 Secondary DNS:                  172.28.12.20
28 IP4 route 1 IP:                 None
29 IP4 route 1 gateway:            None
30 IP4 route 1 mask:               None
31 IP4 route 2 IP:                 None
32 IP4 route 2 gateway:            None
33 IP4 route 2 mask:               None
34 IP6 address:                    None
35 IP6 prefix length:              None
36 IP6 global gateway:             None
37 IP6 link local addr:            None
38 IP6 route 1 dest:               None
39 IP6 route 1 pref len:           None
40 IP6 route 1 gateway:            None
41 IP6 route 2 dest:               None
42 IP6 route 2 pref len:           None
43 IP6 route 2 gateway:            None
44 MAC address:                    001ae809312a
45 LLDP:                           Yes
46 VLAN discovery:                 DHCP
```

3.23.3 User Access to Diagnostic Information

If this option is enabled, extended phone data is also displayed to the user. To view the data, the user must click on the "Diagnostic information" link in the user menu.

INFO: The Diagnostic Information can also be viewed by the user on the local phone by selecting **User > Diagnostic information**.

Administration via WBM

Diagnostics > Diagnostic information > User access

3.23.4 Diagnostic Call

The feature "Rapid Status Diagnostic Call" will provide the possibility to place a diagnostic call, for example by the user, which starts call related tracing on the phone and on involved OpenScape Voice and collect these traces at OpenScape Voice Trace Manager (OSVTM). With all these traces available, a call can be followed throughout the voice system and a possible problem can be detected faster. As all traces from all involved components are available at the first level support, the analysis of a possible problem can be started immediately.

A so-called diagnostic scenario will enable traces on all involved SIP components of the OSC Voice solution and store all traces at a central server. A tool will help service, to follow a call through the traces and determine the point of problem.

The approach is to use a SIP Header ([1]) to indicate, whether a call is a diagnostic call or not. Presence of this header will mean that related call is a diagnostic call. Absence of this field means a non-diagnostic call. This header will either switch on traces in the solution component or be ignored if it isn't supported. If the call is recognized as a diagnostic call, the traces will be sent to DLS as a first step and then DLS will forward them to OSVTM. Collected traces will either be sent after a successful end of diagnostic scenario or if trace file is full.

For enabling tracing on all involved solution components, a call must be recognized to be a "diagnostic" call. Therefore, a special SIP header will be added to the signalling messages. All components which are able to support such a call will then switch on traces and send the traces to DLS server (which will forward them to a pre-defined OSVTM server).

A dial-prefix has been chosen, as the dialed number should be identical to a number, where the user identified a possible problem. This prefix will be filtered before placing a call, so that the SIP messages will be similar to the ones for the problematic destination.

The SIP header "X-Siemens-Trace-ID" has been chosen, as this is a special SIP field created for this feature. Existence of the diagnostic call, start and finish of a diagnostic call can be determined via this field [1].

Trace id will be unique throughout the system and the following format will be used to generate trace id:

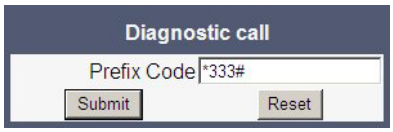
```
TraceId: <UNIX_Timestamp>_<Last 6 bytes of MAC Address>
```

If related calls (diagnostic or not) are established following the start of the diagnostic call, then it turns to be a diagnostic scenario. Related calls become diagnostic (if they are not already) and traces are collected until the last diagnostic call ends plus a predefined timer. This timer guarantees capturing related information regarding to a problematic scenario.

The diagnostic call can only be determined during the call so initial traces might get lost. For this reason, user may need to do additional call. This is completely user related and user should be informed about the process. There will not be any restriction to prevent user to dial the prefix. If the prefix is configured by admin, user can always dial the prefix and start a diagnostic call. The prefix has to consist of the leading asterisk followed by three digits and the hash. Example: *333#.

Administration via WBM

Maintenance > Diagnostic Call



Administration via Local Phone

|--- Admin	
|--- Maintenance	
|--- Diagnostic Call	

Admin will not be able to change trace settings or can not clear the existing phone traces during an active diagnostic tracing. If admin tries to change trace configuration or delete existing traces this will not be allowed and admin will get the following error: **Change not allowed: Diagnostic tracing is active!**

3.23.5 LAN Monitoring

The LAN port mirror facility allows for monitoring all network traffic at the phone's LAN port.

Additionally, there is a possibility to monitor LAN traffic and port settings in the Local user menu:

|--- User	
|--- Network information	
|--- IP address	
|--- WBM URL	
|--- DNS domain	
|--- LAN RX	
|--- LAN TX	
|--- PC RX	
|--- PC TX	
|--- LAN autonegotiated	

|--- LAN information	
|--- PC autonegotiated	
|--- PC information	

3.23.6 LLDP-MED

When the phone is connected to a switch with LLDP-MED capabilities, it can receive a VLAN ID and QoS parameters and advertise its own network-related properties. The data is exchanged in TLV (Type-Length-Value) format.

Both sent and received LLDP-MED data can be monitored at the administrator interface.

> ***INFO:*** For details on LLDP-MED, please refer to the ANSI/TIA-1057 standard.

For a network configuration example that shows LLDP-MED in operation, please refer to *An LLDP-Med Example*.

Displayed Data

- **Extended Power**: Power Consumption; relevant for PoE.
- **Network policy (voice)**: VLAN ID and QoS (Quality of Service) parameters for voice transport.
- **Network policy (signalling)**: VLAN ID and QoS (Quality of Service) parameters for signalling.
- **LLDEP-MED capabilities**: The LLDP-MED TLVs supported by the phone and the switch as well as the specific device class they belong to.
- **MAC_Phy configuration**: Identifies the possible duplex and bit rate capability of the sending device, its current duplex and bit rate capability, and whether theses settings are the result of auto-negotiation during the initialization of the link, or of manual set override actions.
- **System capabilities**: The devices advertise their potential and currently enabled functions, e. g. "Bridge", "Telephone".
- **TTL**: Time To Live. This parameter determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.

View Data From WBM

Diagnostics > LLDEP-MED TLVs

LLDP-MED TLVs

Sent	Received
Sent: Thu Jan 17 13:59:20 2013 Chassis ID TLV Data .Subtype = Network address .IANA_TYPE = IPv4 Address .ID = 172.28.158.205 Port ID TLV Data .Subtype = MAC address .ID = 00:1A:E8:09:31:2A TTL TLV data .seconds = 120 System Caps TLV Data .Supported = Bridge, Telephone, .Enabled = Telephone, MAC_Phy config TLV data .Auto-set supported = Yes .Auto-set enabled = Yes .PMD = 0x6c01 .PMD1 = 10BASE-T half duplex mode .PMD2 = 10BASE-T full duplex mode .PMD3 = 100BASE-TX half duplex mode .PMD4 = 100BASE-TX full duplex mode .PMD5 = 1000BASE-T full duplex mode .MAU = 100BaseTXFD : 0x10 LLDP-MED Caps TLV Data .Caps - LLDP-MED = Yes .Caps - Network Policy = Yes .Caps - Location ID = No .Caps - Extended Power Mdi PD = Yes .Caps - Extended Power Mdi Pse = No .Caps - Inventory = No .Type = Endpoint Class III Network policy (Voice) TLV data .Policy unknown = No .Tagged = Yes .VLAN ID = 548 .Layer 2 priority = 5 .DSCP = 46	Received: Thu Jan 17 13:59:20 2013 TTL TLV data .seconds = Network policy .TLV not available

View Data From Local Menu

If both sent and received values are concordant, **OK** is appended to the parameter. If not, an error message is displayed.

|--- Admin	
|--- Network	
|--- LLDP-MED operation	
|--- Extended Power	
|--- Network policy (voice)	
|--- LLDEP-MED cap's	

|--- MAC_Phy config	
|--- System cap's	
|--- TTL	

3.23.7 IP Tests

For network diagnostics, the OpenScape Desk Phone can ping any host or network device to determine whether it is reachable. Additionally, the IP route to a host or network device can be traced using the traceroute tool contained in the phone software.

The **Pre Defined Ping tests** provide pinging for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

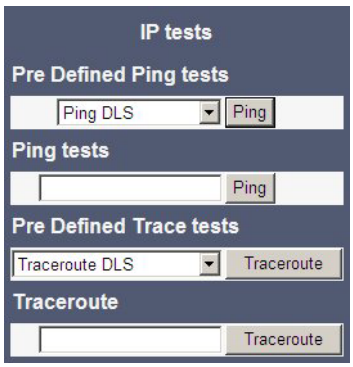
Ping tests enables the pinging of a random IP address.

The **Pre Defined Trace tests** provide traceroute tests for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

Traceroute enables traceroute tests for a random IP address.

Administration via WBM

Diagnostics > Miscellaneous > IP tests



3.23.8 Process and Memory Information

The processes currently running on the phone's operating system as well as their CPU and memory usage can be monitored here. 100 processes are monitored on the web page. For further information, please refer to the manual of the "top" command for Unix/Linux systems, or to related documentation.

The amount of free memory is checked on a regular basis in order to prevent problems caused by low memory. This check determines whether a recovery is necessary.

When **Disable reboot** is checked, no reboot will take place when a memory problem has been found. However, recovery requires a reboot.

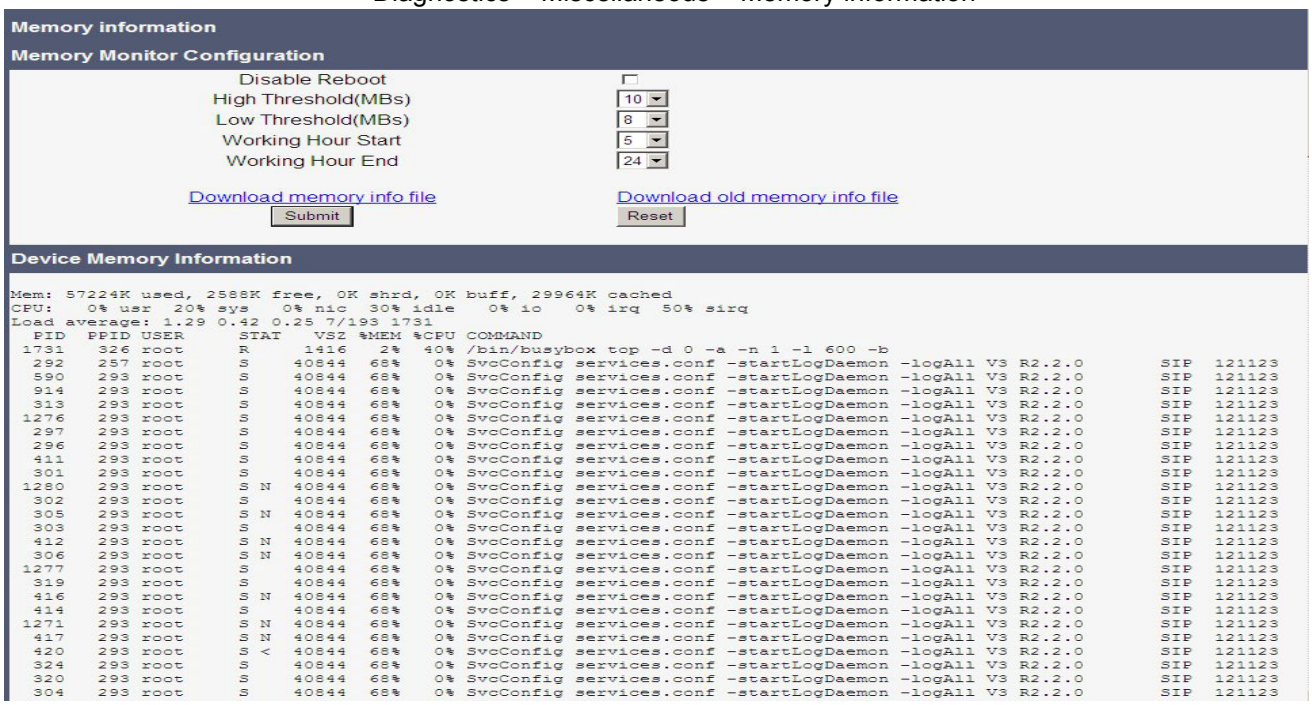
The recovery process will be triggered when the available main memory (RAM) falls below a given threshold value. As memory consumption is assumed to be higher during working hours, two thresholds are configurable. The **High Threshold (MBs)** parameter defines the threshold for off-time. For the OpenScape Desk Phone IP 35G, the default value is 10 MB, and for the OpenScape Desk Phone IP 55G, it is 30 MB. With **Low Threshold (MBs)**, the threshold for off-time is defined. For the OpenScape Desk Phone IP 35G, the default value is 8 MB, and for the OpenScape Desk Phone IP 55G, it is 20 MB.

The beginning and end of the working hours are defined in 24 hours format with **Working Hour Start** (Default: 5) and **Working Hour End** (Default: 24).

When memory shortage has occurred, information about the incident is written to a log file which can be viewed via the **Download memory info file** link. If there has been a previous case of memory shortage, the corresponding log file can be viewed via **Download memory info file**.

Administration via WBM

Diagnostics > Miscellaneous > Memory information



3.23.9 Fault Trace Configuration

Error tracing and logging can be configured separately for all components, i. e. the services and applications running on the OpenScape Desk Phone. The resulting files can be viewed in the WBM web pages over the **Download** links.

The **File size (bytes)** parameter sets the maximum file size. When it is reached, the data is saved as old file, and a new file is generated. From then on, the trace data is written to the new file. When the maximum file size is reached again, the data is saved as old file once more, thereby overwriting the previous old file. The default value is 65536.

> ***INFO:*** The absolute maximum file size is 3 000 000 bytes. However, on OpenScape Desk Phones, a maximum size no greater than 1000 000 bytes is recommended due to the amount of available memory.

The **Trace timeout (minutes)** determines when to stop tracing. When the timeout is reached, the trace settings for all components are set to OFF, but ERROR and STATUS messages are still written to the trace file ad infinitum. When the trace file has reached its maximum size, the data is saved, and a new file is created (for more information, see **File size (bytes)** above). If the value is 0, the trace data will be written without time limit.

If **Automatic clear before start** is checked, the existing trace file will be deleted on pressing the **Submit** button, and a new, empty trace file will be generated. By default, it is unchecked.

You can read the log files by clicking on the appropriate hyperlinks (the hyperlinks work only if the file in question has been created). The following logs can be viewed:

- **Download trace file**
  The trace data according to the settings specified for the services.
- **Download boot file**
  The system messages of the booting process. These messages are incorporated in the syslog file (see *Download syslog file* underneath).
- **Download saved trace file**
  Normally, the trace file is saved only in the phone RAM. When the phone restarts in a controlled manner, the trace file will be saved in permanent memory.
- **Download saved boot file**
  Normally, the boot file is saved only in the phone RAM. When the phone restarts in a controlled manner, the boot file will be saved in permanent memory. These messages are incorporated in the syslog file (see *Download syslog file* underneath).
- **Download upgrade trace file**
  The trace log created during a software upgrade.
- **Download upgrade error file**
  The error messages created during a software upgrade. These messages are incorporated in the syslog file (see Download syslog file underneath).
- **Download exception file**
  If an exception occurs in a process running on the phone, a message is written to this file. These messages are incorporated in the syslog file (see *Download syslog file* underneath).

- **Download old exception file**
  The exception file is stored permanent memory. When the file has reached its size limit, it will be saved as old exception file, and the current exception file is emptied for future messages. The old exception file can be viewed here.
- **Download old trace file**
  The trace file is stored in permanent memory. When the file has reached its size limit, it will be saved as old trace file, and the current exception file is emptied for future messages. The old trace file can be viewed here.
- **Download error file**
  All error messages the phone has created, according to the settings for the individual services.
  Additional log messages are issued for the following scenarios:
  - Update has been allowed due to override flag being set
  - Whole part number is not recognised
  - Block 4 of part number is not recognised
  - Downloaded software does not have a hardware level included
- **Download syslog file**
  Messages from the phone's operating system, including error and exception messages.
- **Download old syslog file**
  Old messages from the phone's operating system.
- **Download saved syslog file**
  Saved messages from the phone's operating system.
- **Download Database file**
  Configuration parameters of the phone in SQLite format.
- **Download HPT remote service log file**
  Log data from the HPT service.
- **Download dial plan file**
  If a dial plan has been uploaded to the phone, it is displayed here, along with its status (enabled/disabled) and error status. For details, please refer to *Dial Plan* and *Example Dial Plan*.

By pressing **Submit**, the trace settings are submitted to the phone. With **Reset**, the recent changes can be canceled.

The following trace levels can be selected:

- **OFF**: Default value. Only error messages are stored.
- **ERROR**: Error messages are stored.
- **TRACE**: Trace messages are stored. These contain detailed information about the processes taking place in the phone.
- **DEBUG**: All types of messages are stored.

Brief Descriptions of the Components/Services

- **Administration**
  Deals with the changing and setting of parameters within the phone database, from both the User and Admin menus.

- **Application framework**
  All applications within the phone, e.g. Call view, Call log or Phonebook, are run within the application framework. It is responsible for the switching between different applications and bringing them into and out of focus as appropriate.
- **Call log**
  The Call log application displays the call history of the phone.
- **Call view**
  Handles the representation of telephony calls on the phone screen.
- **Certificate management**
  Handles the verification and exchange of certificates for security and verification purposes.
- **Clock service**
  Handles the phone's time and date, including daylight saving and NTP functionality.
- **Communications**
  Involved in the passing of call related information and signaling to and from the CSTA service.
- **Component registrar**
  Handles data relating to the type of phone, e.g. OpenScape Desk Phone IP 35G, OpenScape Desk Phone IP 55G.
- **CSTA service**
  Any CSTA messages are handled by this service. CSTA messages are used within the phone by all services as a common call progression and control protocol.
- **Data Access service**
  Allows other services to access the data held within the phone database.
- **Desktop**
  Responsible for the shared parts of the phone display. Primarily these are the status bar at the top of the screen and the FPK labels.
- **Digit analysis service**
  Analyses and modifies digit streams which are sent to and received by the phone, e.g. canonical conversion.
- **Directory service**
  Performs a look up for data in the phonebook, trying to match incoming and outgoing numbers with entries in the phonebook.
- **DLS client management**
  Handles interactions with the DLS (Deployment Service).
- **Health service**
  Monitors other components of the phone for diagnostic purposes and provides a logging interface for the services in the phone.
- **Help**
  Handles the help function.
- **Instrumentation service**
  Used by the Husim phone tester to exchange data with the phone for remote control, testing and monitoring purposes.

- **Journal service**
  Responsible for saving and retrieving call history information, which is used by the Call log application.
- **Media control service**
  Provides the control of media streams (voice, tones, ringing etc.) within the phone.
- **Media processing service**
  This is a layer of software between the media control service, the tone generation, and voice engine services. It is also involved in the switching of audio devices such as the handset and loudspeaker.
- **Media recording service**
  Logs the data flow generated with call recording.
- **Mobility service**
  Handles the mobility feature whereby users can log onto different phones and have them configured to their own profile.
- **OpenStage client management**
  Provides a means by which other services within the phone can interact with the database.
- **Performance Marks**
  Aid for measuring the performance of the phone. For events triggered by the user, a performance mark is written to the trace file, together with a timestamp in the format hh:mm:ss yyyy.milliseconds, and information about the event. The time span between two performance marks is an indicator for the performance of the phone.

  INFO: The trace level must be set to "TRACE" or "DEBUG".

- **Password management service**
  Verifies passwords used in the phone.
- **Phonebook**
  Responsible for the Phonebook application.
- **Physical interface service**
  Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, clickwheel and slider.
- **Service framework**
  This is the environment within which other phone services operate. It is involved in the starting and stopping of services.
- **Service registry**
  Keeps a record of all services currently running inside the phone.
- **Sidecar service**
  Handles interactions between the phone and any attached sidecars.
- **SIP call control**
  Contains the call model for the phone and is associated with telephony and call handling.

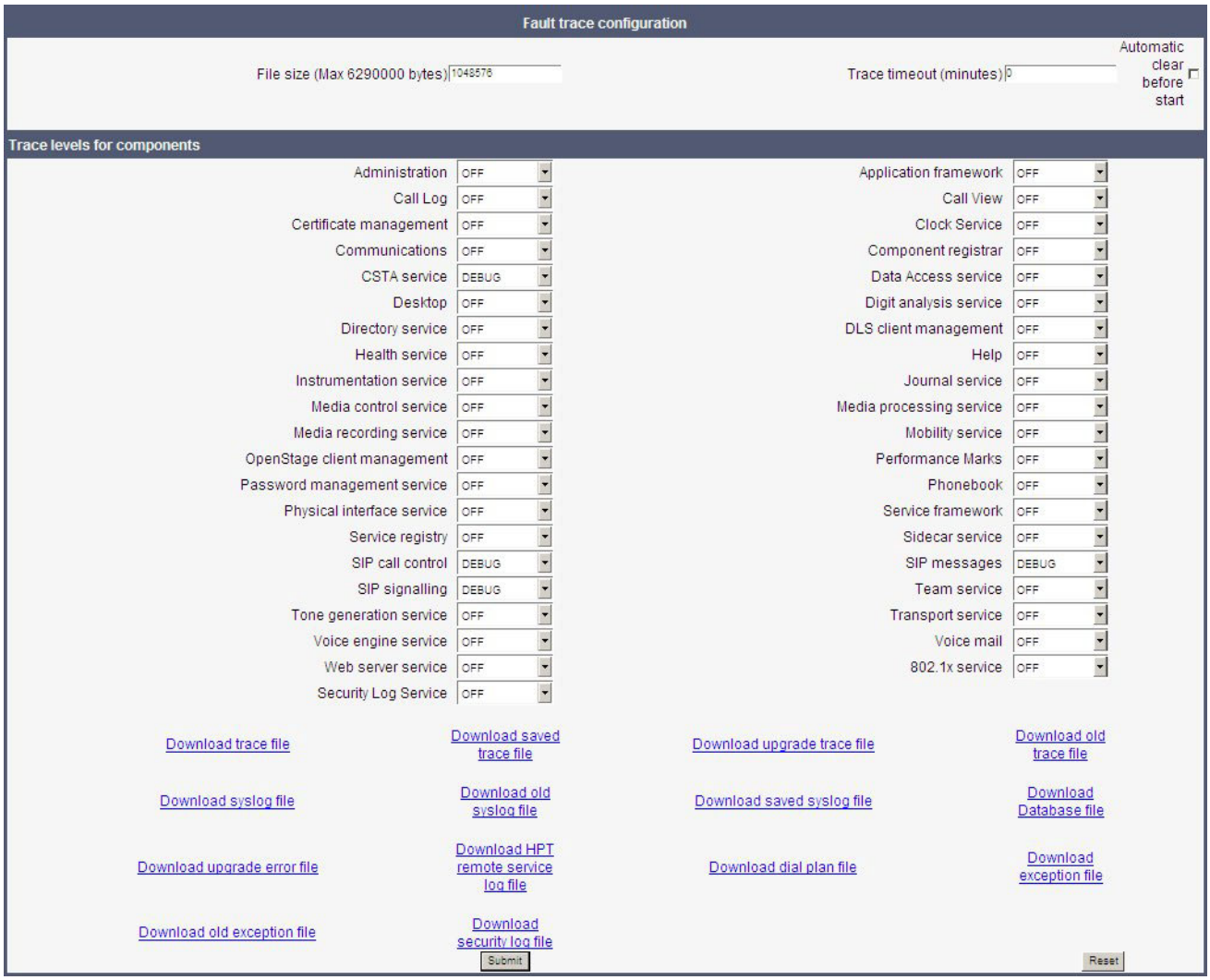
- **SIP messages**
  Traces the SIP messages exchanged by the phone.

  INFO: After changing the level for the tracing of SIP messages, the phone must be rebooted. Otherwise the changes would have no effect.

- **SIP signalling**
  Involved in the creation and parsing of SIP messages. This service communicates directly with the SIP stack.
- **Team Service**
  Primarily concerned with keyset operation.
- **Tone generation service**
  Handles the generation of the tones and ringers on the phone.
- **Transport service**
  Provides the IP (LAN) interface between the phone and the outside world.
- **Voice engine**
  Provides a switching mechanism for voice streams within the phone. This component is also involved in QDC, Music on hold and voice instrumentation.
- **Voice mail**
  Handles the voice mail functionality.
- **Web server service**
  Provides access to the phone via web browser.
- **802.1x service**
  Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points.
- **Security Log Service**

Administration via WBM

Diagnostics > Fault Trace Configuration



3.23.10 Easy Trace Profiles

In order to simplify tracing for a specific problem, the tracing levels can be adjusted using predefined settings.

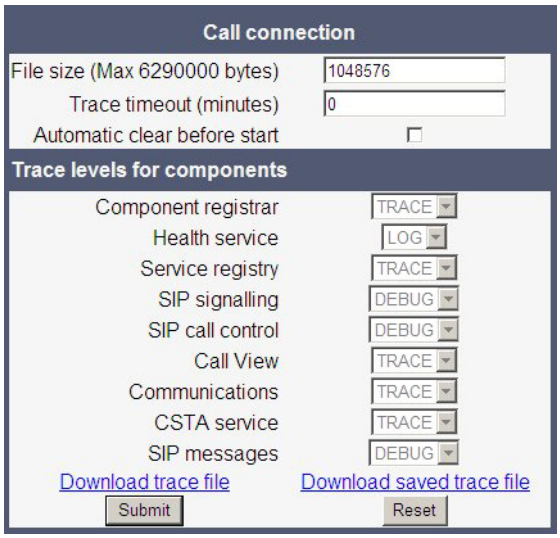
The Easy Trace Profiles provide settings for a specific area, e. g. call connection. On pressing Submit, those pre-defined settings are sent to the phone. If desired, the settings can be modified anytime using the general mask for trace configuration under Diagnostics > Fault Trace Configuration (see *Fault Trace Configuration*).

If desired, the tracing for all services can be disabled (see *Clear All Profiles (No Tracing for All Services)*).

The following sections describe the Easy Trace Profiles available for the phone.

3.23.10.1 Call Connection

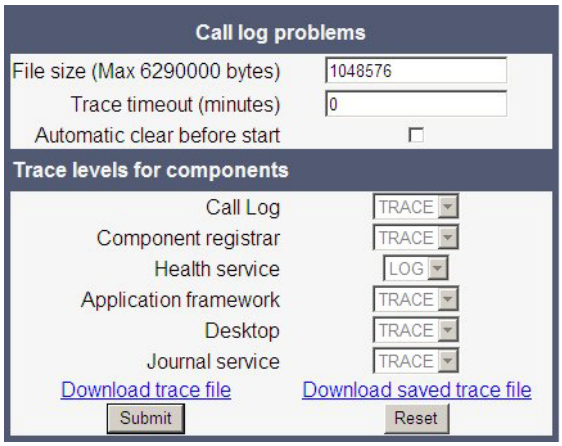
Diagnostics > Easy Trace Profiles > Call connection



INFO: This Easy Trace profile contains the tracing of SIP messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

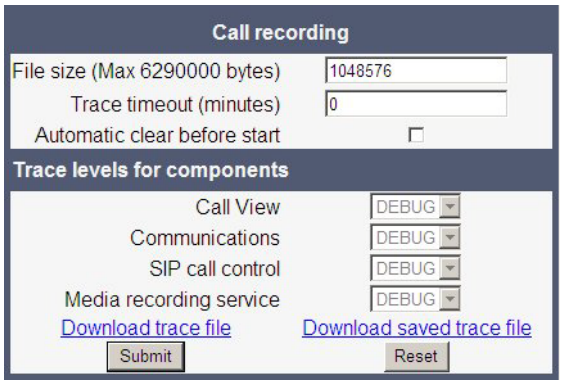
3.23.10.2 Call Log

Diagnostics > Easy Trace Profiles > Call log problems



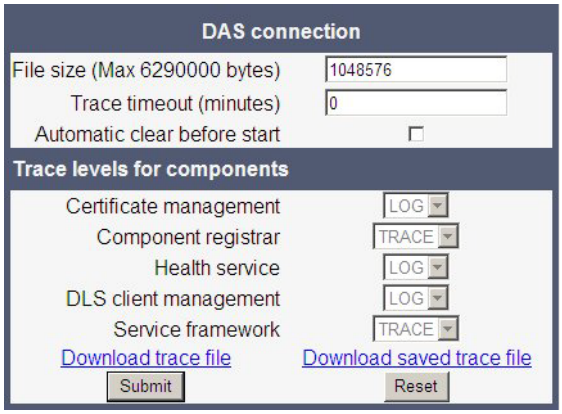
3.23.10.3 Call Recording

Diagnostics > Easy Trace Profiles > Call recording



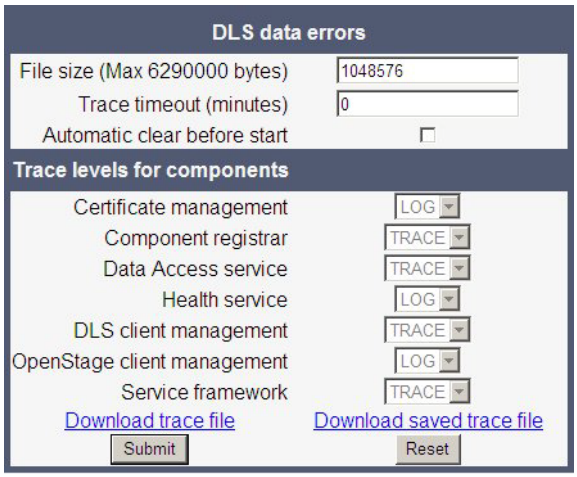
3.23.10.4 DAS Connection

Diagnostics > Easy Trace Profiles > DAS connection



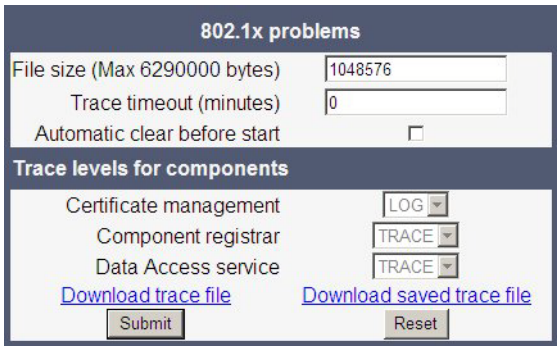
3.23.10.5 DLS Data Errors

Diagnostics > Easy Trace Profiles > DLS data errors



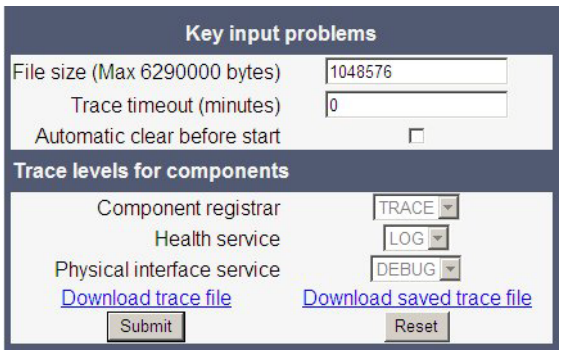
3.23.10.6 802.1x

Diagnostics > Easy Trace Profiles > 802.1x



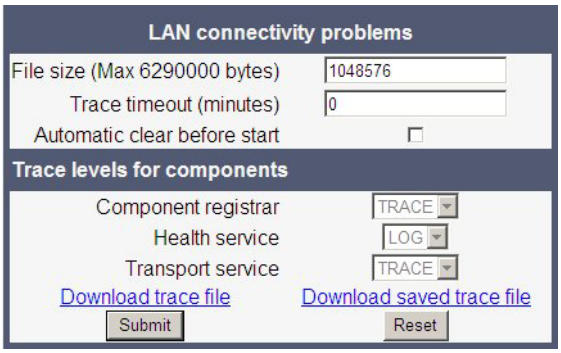
3.23.10.7 Key Input

Diagnostics > Easy Trace Profiles > Key input problems



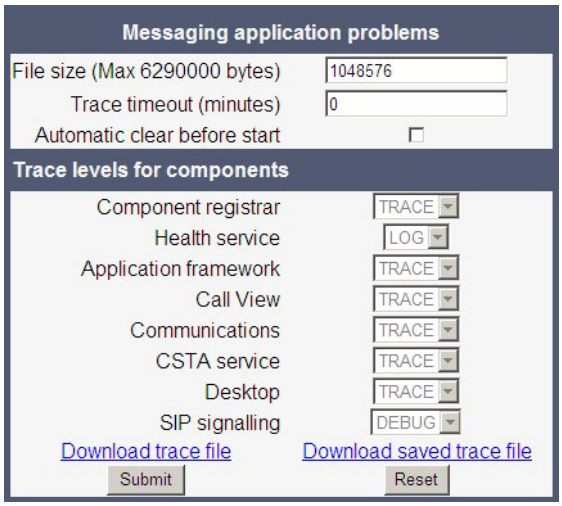
3.23.10.8 LAN Connectivity

Diagnostics > Easy Trace Profiles > LAN connectivity problems



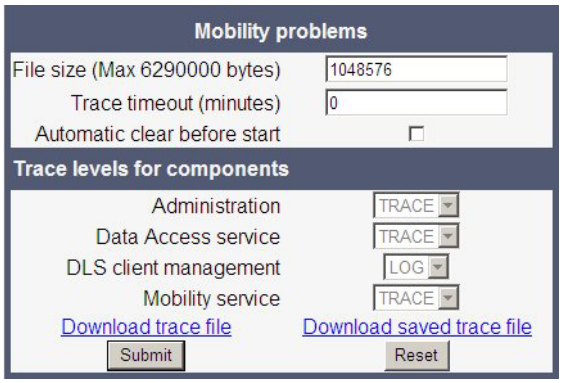
3.23.10.9 Messaging

Diagnostics > Easy Trace Profiles > Messaging application problems



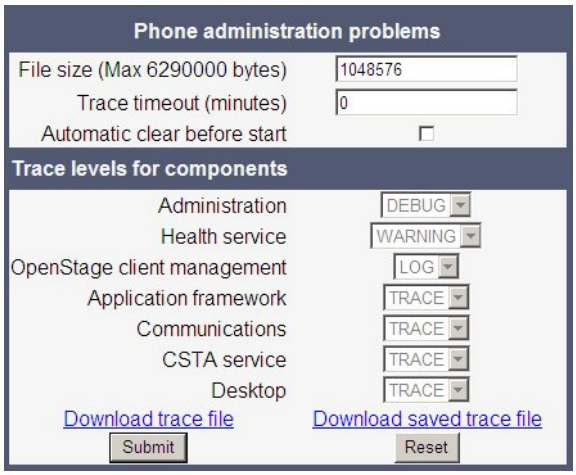
3.23.10.10 Mobility

Diagnostics > Easy Trace Profiles > Mobility problems



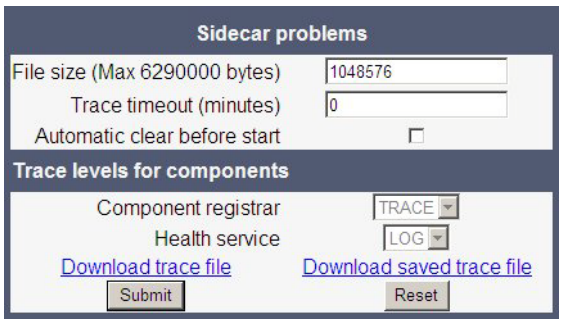
3.23.10.11 Phone administration

Diagnostics > Easy Trace Profiles > Phone administration problems



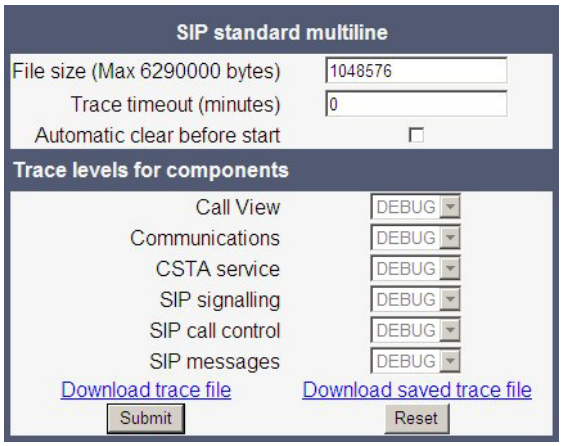
3.23.10.12 Sidecar

Diagnostics > Easy Trace Profiles > Sidecar problems



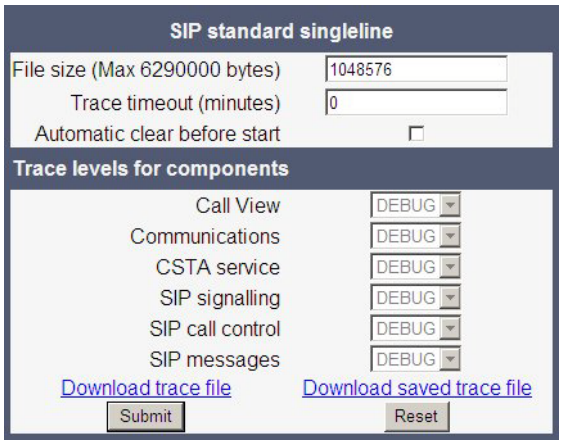
3.23.10.13 SIP Standard Multiline

Diagnostics > Easy Trace Profiles > SIP Standard Multiline problems



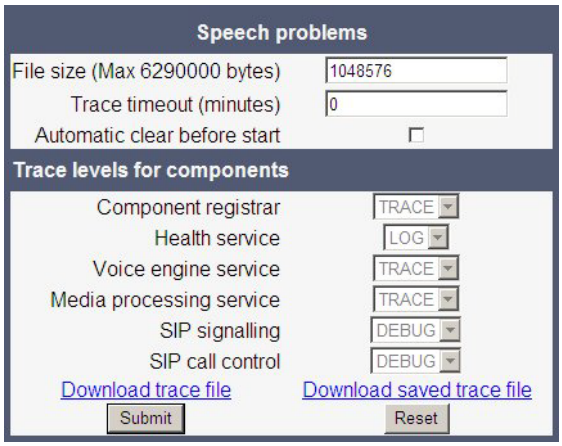
3.23.10.14 SIP Standard Single Line

Diagnostics > Easy Trace Profiles > SIP Standard Singleline



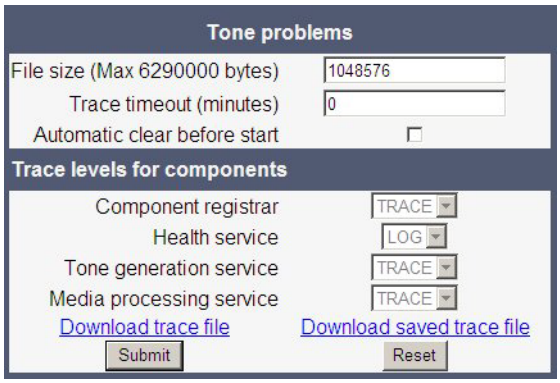
3.23.10.15 Speech

Diagnostics > Easy Trace Profiles > Speech problems



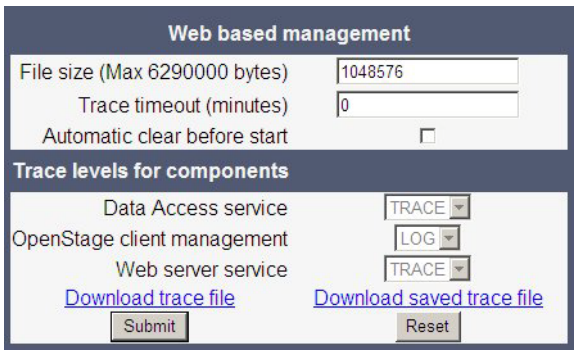
3.23.10.16 Tone

Diagnostics > Easy Trace Profiles > Tone problems



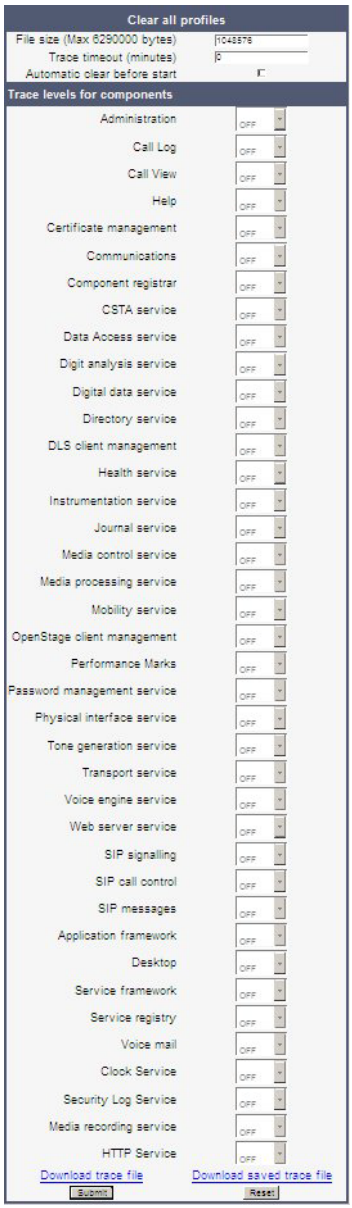
3.23.10.17 Web Based Management

Diagnostics > Easy Trace Profiles > Web based management



3.23.10.18 Clear All Profiles (No Tracing for All Services)

Diagnostics > Easy Trace Profiles > Clear all profiles



3.23.11 QoS Reports

3.23.11.1 Conditions and Thresholds for Report Generation

INFO: For details about the functionality, please refer to the Release Notes.

The generation of QoS (Quality of Service) reports which are sent to a QCU server (see *SNMP*) is configured here.

Data required

- **Report mode**: Sets the conditions for generating a QoS report. Value range:
  - "OFF": No reports are generated.
  - "EOS Threshold exceeded": Default value. A report is created if a) a telephone conversation longer than the Minimum session length has just ended, and b) a threshold value has been exceeded during the conversation.
  - "EOR Threshold exceeded": A report is created if a) the report interval has just passed, and b) a threshold value has been exceeded during the observation interval.
  - "EOS (End of Session)": A report is created if a telephone conversation longer than the Minimum session length has just ended.
  - "EOR (End of Report Interval)": A report is created if the report interval has just passed.
- **Report interval (seconds)**: Time interval between the periodical observations.
  Default: 60
- **Observation interval (seconds)**: During this time interval, the traffic is observed.
  Value: 10
- **Minimum session length (100 millisecond units)**: When the Report mode is set to "EOS Threshold exceeded" or "EOS (End of Session)", a report can be created only if the duration of the conversation exceeds this value.
  Default: 20
- **Maximum jitter (milliseconds)**: When the jitter exceeds this value, a report is generated.
  Default: 20
- **Average round trip delay (milliseconds)**: When the average round trip time exceeds this value, a report is generated.
  Default: 100

Non-compressing codecs / Compressing codecs:

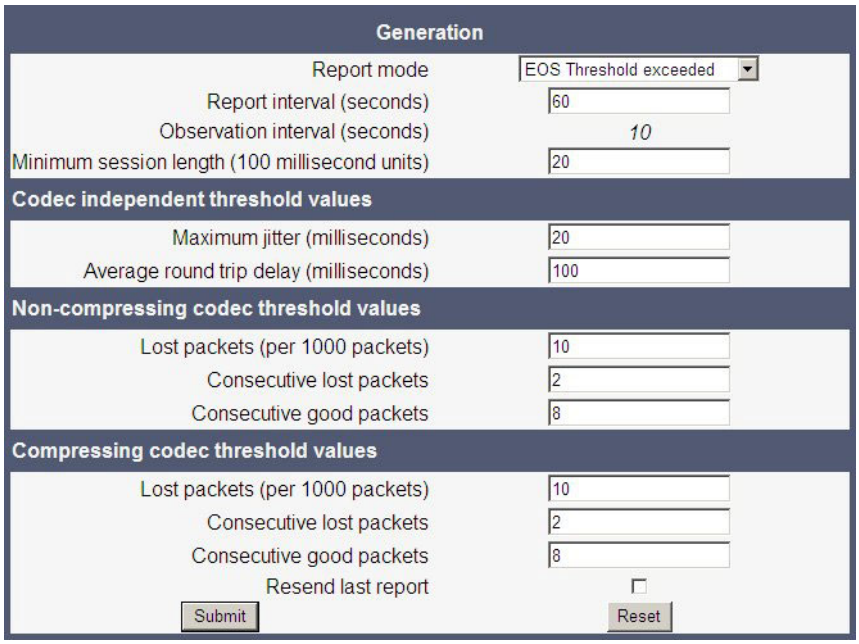
- **Lost packets (per 1000 packets)**: When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
  Default: 10

- **Consecutive lost packets**: When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created.
  Default: 2
- **Consecutive good packets**: When the number of good packets following one another falls below this minimum value, a report is created. Default: 8
- **Resend last report**: If checked, the previous report is sent once again on pressing **Submit**.
  Value range: "Yes", "No"
  Default: "No"

The transmission of report data can be triggered manually by pressing **Send now** in the local menu.

Administration via WBM

Diagnostics > QoS Reports > Generation



Administration via Local Phone

|--- Admin	
|--- Network	
|--- QoS	
|--- Reports	
|--- Generation	
| |--- Mode	
| |--- Report interval	
| |--- Observe interval	

| |--- Minimum session length	
|--- Send now	
|--- Thresholds	
|--- Maximum jitter	
|--- Round-trip delay	
|--- Non-compressing:	
|--- ...Lost packets (K)	
|--- ...Lost consecutive	
|--- ...Good consecutive	
|--- Compressing:	
|--- ...Lost packets (K)	
|--- ...Lost consecutive	
|--- ...Good consecutive	

3.23.11.2 View Report

OpenScape Desk Phones generate QoS reports using a HiPath specific format, QDC (QoS Data Collection). The reports created for the last 6 sessions, i. e. conversations, can be viewed on the WBM.

To enable the generation of reports, please ensure that:

- the switch QoS traps to QCU (System > SNMP) is activated (see *SNMP*);
- the conditions for the generation of reports are set adequately (see*Conditions and Thresholds for Report Generation*).

For details about QoS reports on HiPath devices, see the *HiPath QoS Data Collection V 1.0 Service Manual*.

A QoS report contains the following data:

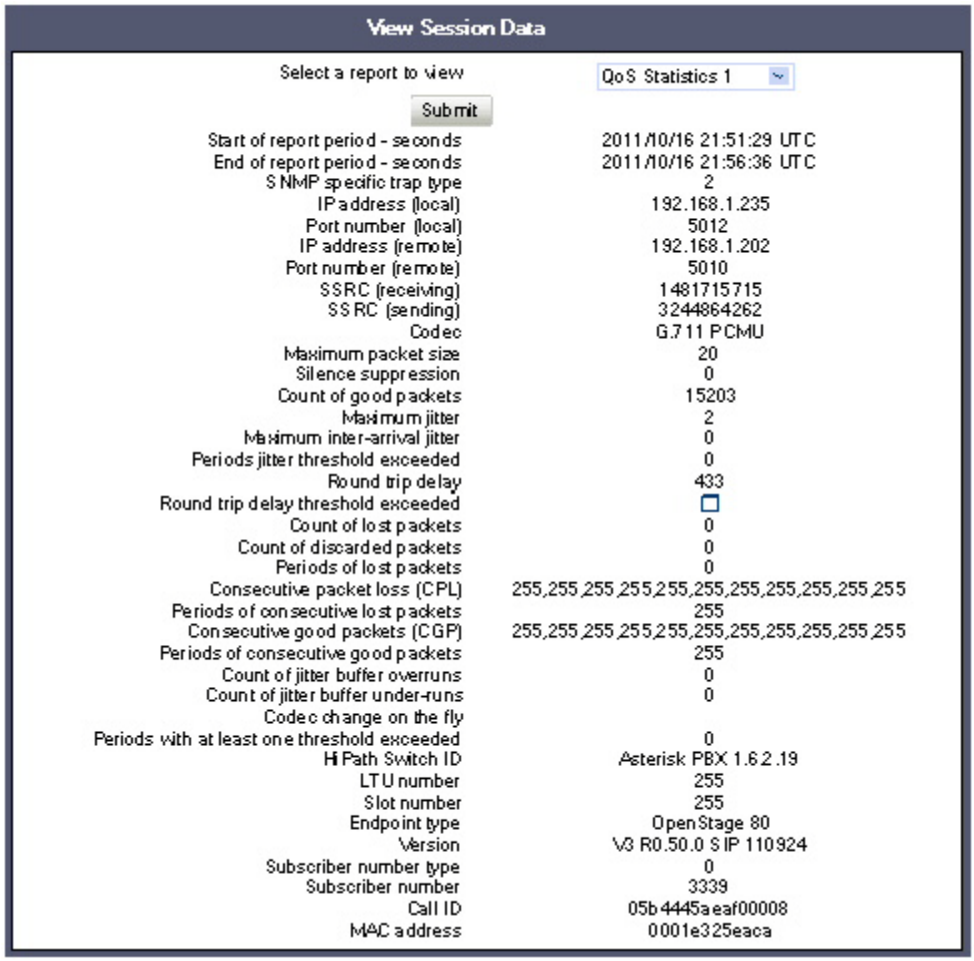
- **Start of report period - seconds**: NTP time in seconds for the start of the report period.
- **Start of report period - fraction of seconds**: Additional split seconds to be added to the seconds for an exact start time.
- **End of report period - seconds**: NTP time in seconds for the end of the report period.
- **End of report period - fraction of seconds**: Additional split seconds to be added to the seconds for an exact end time.
- **SNMP specific trap type**: The trap type is a 5 bit value calculated from a list of threshold-exceeding bits. Every time a threshold is exceeded, the associated bit is set, otherwise it is cleared.
  The trace type bits are defined as follows:
  - Bit 0: Jitter threshold was exceeded.
  - Bit 1: Delay threshold was exceeded.

  - Bit 2: Threshold for lost packets was exceeded.
  - Bit 3: Threshold for consecutive lost packets was exceeded.
  - Bit 4: Threshold for consecutive good packets was exceeded.
- **IP address (local)**: IP address of the local phone.
- **Port number (local)**: RTP receiving port of the local phone.
- **IP address (remote)**: IP address of the remote phone that took part in the session.
- **Port number (remote)**: RTP sending port of the local phone.
- **SSRC (receiving)**: RTP Source Synchronization Identifier of the local phone.
- **SSRC (sending)**: RTP Source Synchronization Identifier of the remote phone.
- **Codec**: Number of the Payload Type applied in the session; see RFC 3551 (Table 4 and 5).
- **Maximum packet size**: Maximum size (in ms) of packets received during the report interval.
- **Silence suppression**: Number of silence suppression activation objects found in the RTP stream received. A silence suppression activation object is defined as a period of silence when no encoded voice signals were transmitted by the sender.
- **Count of good packets**: Total amount of good packets.
- **Maximum jitter**: Maximum jitter (in ms) found during the report interval.
- **Maximum inter-arrival jitter**: Maximum of the inter-arrival jitter values (in ms). The inter-arrival jitter is the smoothed absolute value of the jitter measurements. It is calculated continuously. For details about the calculation, see RFC 3550.
- **Periods jitter threshold exceeded**: Number of observation intervals in which the threshold for maximum jitter was exceeded.
- **Round trip delay**: Average value of delay calculated for each RTCP packet. The first value is available after about 15 sec.
- **Round trip delay threshold exceeded**: Set to "true" if the average round trip delay -threshold value was exceeded in the report interval.
- **Count of lost packets**: Number of packets lost in the course of speech decoding.
- **Count of discarded packets**: Number of the packets discarded without transferring the contents.
- **Periods of lost packets**: Number of observation intervals in which the threshold for lost packets was exceeded.
- **Consecutive packet loss (CPL)**: List of sequences consecutive packets that were all lost, grouped according to the amount of packets per sequence. The first number in the list counts single lost packets, the second number counts sequences of two lost packets, and so on. The last number counts sequences of more than 10 lost packets.
- **Periods of consecutive lost packets**: Number of observation intervals in which the threshold for consecutive lost packets was exceeded.

- **Consecutive good packets (CGP)**: List of sequences consecutive packets that were all processed, grouped according to the amount of packets per sequence. The first number in the list counts single good packets, the second number counts sequences of two good packets, and so on. The last number counts sequences of more than 10 good packets. All values are reset to 0 after an interval without packet loss.
- **Periods of consecutive good packets**: Number of intervals in which the count of lost packets went below the threshold.
- **Count of jitter buffer overruns**: Number of packets rejected because the jitter buffer was full.
- **Count of jitter buffer under-runs**: Increased by one whenever the decoder requests new information on decoding and finds an empty jitter buffer.
- **Codec change on the fly**: The value is 1, if there has been a codec or SSRC change during the observation period, and 0, if there has been no change.
- **Periods with at least one threshold exceeded**: Number of observation intervals with at least one threshold exceedance. If there is no data, the value is 255. The threshold values included are:
  - maximum jitter;
  - lost packets;
  - consecutive lost packets;
  - consecutive good packets.
- **HiPath Switch ID**: Unique number identifying the HiPath switch to which the endpoints are assigned.
- **LTU number**: In HiPath 4000 only, the shelf identification is taken from the shelf containing a gateway.
- **Slot number**: The slot number where the phone is connected in the shelf.
- **Endpoint type**: Type of the local phone.
- **Version**: Software version of the local phone.
- **Subscriber number type**: Type of subscriber number assigned to the local phone. The possible types are:
  - 1: local number, extension only
  - 2: called number, network call
  - 3: E.164 number of the local phone
- **Subscriber number**: Subscriber number of the local phone.
- **Call ID**: SIP call id.
- **MAC address**: MAC address of the local phone.

Data viewing via WBM

Diagnostics > QoS reports > View Session Data



View Session Data

Select a report to view: QoS Statistics 1

Submit

Start of report period - seconds	2011/10/16 21:51:29 UTC
End of report period - seconds	2011/10/16 21:56:36 UTC
SNMP specific trap type	2
IP address (local)	192.168.1.235
Port number (local)	5012
IP address (remote)	192.168.1.202
Port number (remote)	5010
SSRC (receiving)	1481715715
SSRC (sending)	3244864262
Codec	G.711 PCMU
Maximum packet size	20
Silence suppression	0
Count of good packets	15203
Maximum jitter	2
Maximum inter-arrival jitter	0
Periods jitter threshold exceeded	0
Round trip delay	433
Round trip delay threshold exceeded	☐
Count of lost packets	0
Count of discarded packets	0
Periods of lost packets	0
Consecutive packet loss (CPL)	255,255,255,255,255,255,255,255,255,255,255,255
Periods of consecutive lost packets	255
Consecutive good packets (CGP)	255,255,255,255,255,255,255,255,255,255,255,255
Periods of consecutive good packets	255
Count of jitter buffer overruns	0
Count of jitter buffer under-runs	0
Codec change on the fly	
Periods with at least one threshold exceeded	0
HiPath Switch ID	Asterisk PBX 1.6.2.19
LTU number	255
Slot number	255
Endpoint type	OpenStage 80
Version	V3 R0.50.0 SIP 110924
Subscriber number type	0
Subscriber number	3339
Call ID	05b4445aeaf00008
MAC address	0001e325eaca

3.23.12 Core dump

If **Enable core dump** is checked, a core dump will be initiated in case of a severe error. The core dump will be saved to a file. By default, this function is activated.

When **File size unlimited** is checked, there is no size limit for the core dump file. By default, it is not checked.

The maximum size for core dump files in MBytes can be chosen in the **Limited file size (MBs)** field. The possible values are 1, 5, 10, 25, 50, 75, and 100. The default value is 100.

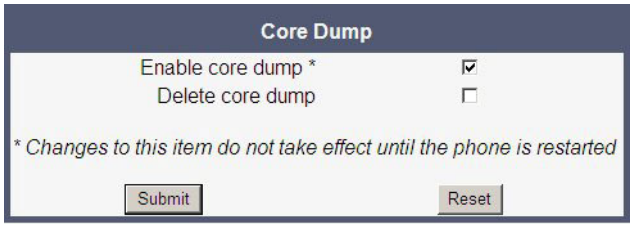
> ***INFO:*** Unlimited file size is preset, and the parameters **File size unlimited** as well as **Limited file size (MBs)** are not available.

If **Delete core dump** is activated, the current core dump file is deleted on **Submit**. By default, this is not activated.

If one or more core dump file exist, hyperlinks for downloading will be created automatically.

Administration via WBM

Diagnostics > Miscellaneous > Core dump



3.23.13 Remote Tracing – Syslog

All trace messages created by the components of the phone software can be sent to a remote server using the syslog protocol. This is helpful especially for long-term observations with a greater number of phones.

To enable remote tracing, **Remote trace status** must be set to "Enabled". Furthermore, the IP address of the server receiving the syslog messages must be entered in **Remote Server**, and the corresponding server port must be given in **Remote Server Port**.

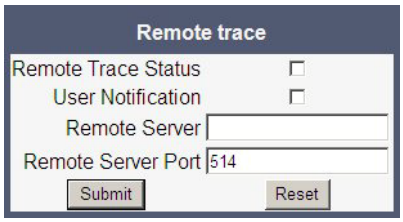
The **User Notification** parameter controls whether the user is notified about the remote tracing or not. If user notification is enabled, a blinking symbol (on OpenScape Desk Phone IP 55G; on OpenScape Desk Phone IP 35G) will inform the user when remote tracing is active, that is, when **Remote Trace Status** is set to "Enabled".

Administration via Local Phone

|--- Admin	
|--- Maintenance	
|--- Remote trace	
|--- Remote trace status	
|--- User notification	
|--- Remote ip	
|--- Remote port	

Administration via WBM

Maintenance > Remote Trace



3.23.14 HPT Interface (For Service Staff)

For special diagnosis and maintenance tasks, the service staff may employ the HPT tool, which is able to control and observe an OpenScape Desk Phone remotely. For security reasons, this tool can only be used when a dongle key file is uploaded to the phone (see *Dongle Key*). This key is accessible to the service staff only. It is specific for a particular SIP firmware version, but it will also be valid for previous versions.

There are 2 types of HPT sessions: control session and observation session.

A control session allows for activating phone functions remotely. When a control session is established, the following changes will occur:

- The display shows a message indicating that remote service is active.
- Handset, microphone, speaker, headset, and microphone are disabled.

An observation session allows for supervising events on the phone, like, for instance, pressing a key, incoming calls or navigating in the menus. Before an observation session is started, the user is prompted for allowing the observation. During an observation session, the phone operates normally, including loudspeaker, microphone and ringer. Thus, the local user can demonstrate an error towards the service staff that is connected via HPT.

The HPT interface is enabled by downloading the dongle key file to the phone (see *Dongle Key*). It can be disabled via local menu or WBM. Thereby, the dongle key file is deleted. To enable the HPT interface again, the file must be downloaded anew.

The session data is written to a log file on the phone. It can be downloaded from the Diagnostics > Fault trace configuration menu (see*Fault Trace Configuration*).

Administration via WBM (Disable)

Maintenance > HPT interface

3.24 MWI LED

This configurable item allows the administrator to control how new Voice Mails are indicated to the user - via the **Messages** key LED only, or via the Alert Bar LED only, or via both LEDs.

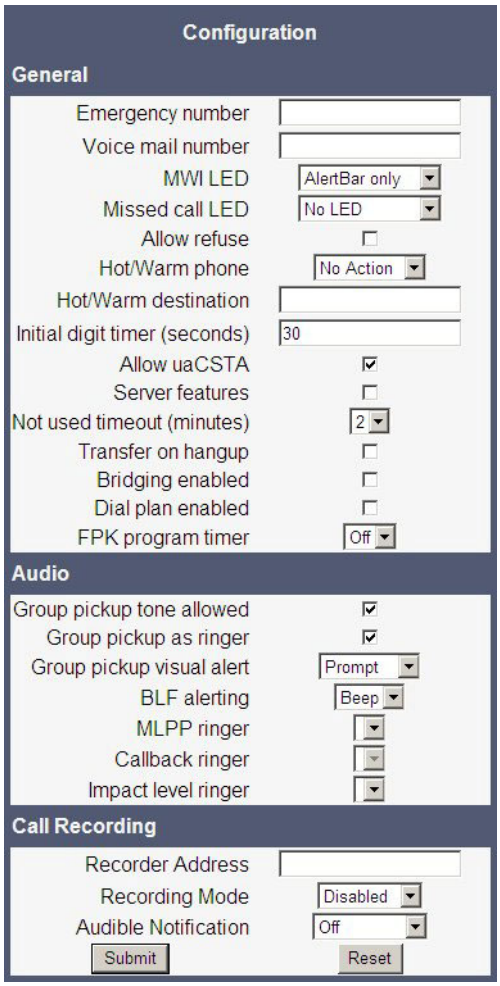
The selection field offers the choice between:

- "Key only" (default)
- "Key & AlertBar"
- "AlertBar only"

Default setting is "**AlertBar only**". After a factory reset, the system will be reset to this value.

Administration via WBM

System > Features > Configuration > MWI LED



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- MWI LED	

3.25 Missed Call LED

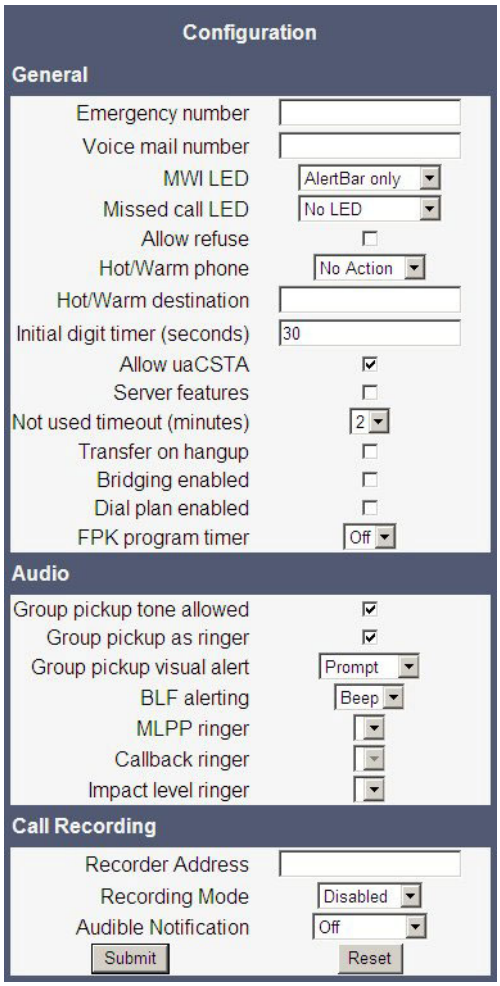
This configurable item allows the administrator to control how new Missed Calls are indicated to the user - via the **Messages** key LED only, via the Alert Bar LED only, via both LEDs, or No LED.

The selection field offers the choice between:

- "Key only"
- "Key & AlertBar"
- "AlertBar only"
- "No LED" (default)

Administration via WBM

System > Features > Configuration > Missed call LED



Administration via Local Phone

|--- Admin	
|--- System	
|--- Features	
|--- Configuration	
|--- General	
|--- Missed call LED	

3.26 Impact Level Notification

Communications for the Public Sector Network (PSN) is seen as originating from, or terminating to, zones with differing 'impact' levels (the impact level indicates how the phone user should handle the call conversation). The purpose is to notify the OpenScape Desk Phone users when they are connecting or in a call where another party in the call is in a lower Impact Level (IL) zone.

This feature uses a UI mechanism to notify/remind the phone user that the call may require special treatment. This involves special icons, text indications and special audio (ringer or tone as appropriate). There are no restrictions on call handling as a result of any special status for the call.

Thus the Lower IL feature only involves UI changes that are triggered by receiving new SIP headers and affects the following:

- Prompts presented to alert for incoming calls
- Prompts presented to monitor progress for outgoing calls
- Connected call displays
- Call scenarios involving multiple calls
- Retrieving a held call

However, since there are no call restrictions explicit for the Lower IL feature, the solution needs to consider some additional scenarios:

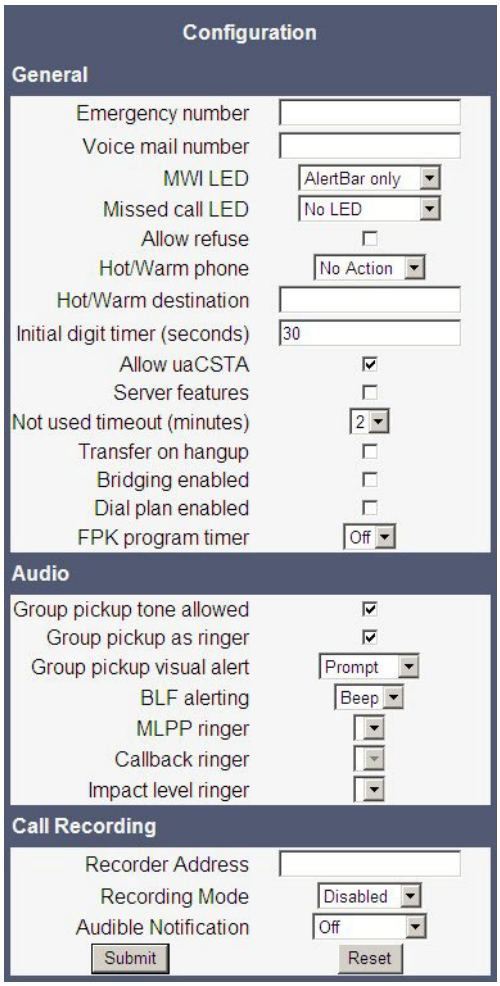
- Group pickup
- Directed pickup
- Callback
- CTI action
- Shared lines on a Keyset

This feature cannot be turned off at the phone since it is driven solely by the OSV.

The OSV is responsible for being aware of the IL of the phone (the phone does not have control of its own level) and the ILs of all other endpoints that are participating in a call with the phone. The OSV uses this information to signal (via a new SIP header) the phone when the call is to be treated as from a lower IL. It may do this during the start of a call or anytime during a call.

Administration via WBM

System > Features > Configuration > Impact level ringer



The phone plays the configured Lower IL ringer when the call is from a Lower IL. The ringer has to be configured in the ringer setting table (see *Distinctive Ringing*).

4 Technical Reference

4.1 Default Port List

The following table contains all default ports, resp. port ranges, and protocols used by the services running on OpenScape SIP phones.

Service	Server Default Port	Client Default Port	Protocol Stack
Payload transport (for 30 lines)	5004 - 5065	5004 - 5065	RTP - RTCP / UDP
SIP subscriber; TCP is used	5060	1024 - 65535	SIP / TCP
SIP subscriber; TLS is used	5061	1024 - 65535	SIP / TLS
SIP subscriber; UDP is used	5060	5060	SIP / UDP
XML applications in -phone, connecting to an application server	---	1024 - 65535	HTTP / TCP
Directory access via LDAP (Only relevant for ??? OpenScape Desk Phone IP 55G ???)	---	1024 - 65535	LDAP / TCP
DHCP Client	---	68	DHCP / UDP
DNS Client	---	1024 - 65535	DNS / TCP_UDP
DLS contact me service - workpoint side	8085	---	HTTP / TCP
Communication with the DLS workpoint interface, default mode	---	18443	HTTPS / TCP - SSL / TLS
Communication with the DLS workpoint interface, secure mode	---	18444	HTTPS / TCP - SSL / TLS
Connection to the control port of FTP server	21	1024 - 65535	FTP / TCP
FTP client; uses the FTP server in active mode	1024 - 65535	20	FTP / TCP
HTTPS file download -server	---	443	HTTPS / TCP - SSL/TLS
Client application which sends QDC data to the QCU	---	1024 - 65535	SNMP / UDP
Sender part of SNMP agent	---	1024 - 65535	SNMP / UDP
Receiver part of SNMP agent; -receives Set/Get commands	161	---	SNMP / UDP
SNTP client; queries time information in unicast operation	---	123	SNTP / UDP

Service	Server Default Port	Client Default Port	Protocol Stack
SNTP client; receives time -information in broadcast operation	123	---	SNTP / UDP
Web server for unencrypted WBM access (up to firmware version V1.4; in higher versions, only encrypted connections are possible)	8085	---	HTTP / TCP
Secure web Server for encrypted WBM access	443	---	HTTPS / TCP - SSL / TLS
OpenScape Phone Manager	65530	---	HTTP / UDP
OpenScape Phone Manager	65531	---	HTTP / TCP

4.2 Troubleshooting: Error Codes

For a set of error cases, specific error codes are defined. These error codes are shown in brackets on the display, following a general error note. Example: „No Telephony possible (LP1)“.

Problem	Description	Error code
Network Problem	No network connection	LI1
Not Initialised	Waiting for data	I1
Unable to use LAN	802.1x error	LX1
Unable to use LAN	Physical connection missing	LP1
Unable to Register	Server timeout	RT2
Unable to Register	Server failed	RF2
Unable to Register	Authentication failed	RA2
Unable to Register	No number configured	RN2
Unable to Register	No server configured	RS2
Unable to Register	No registrar configured	RG2
Unable to Register	No DNS domain configured	RD2
Unable to Register	Rejected by server	RR2
Unable to Register	No phone IP address set	RI2
Survivability	Backup route active	B8
Survivability	Backup not configured	RS8
Survivability	Backup timeout	RT8
Survivability	Backup authentication failed	RA8

INFO: A special “fast-busy” tone (also called congestion tone) is played if a temporary network problem causes a user-initiated call action to fail. Typical call actions: making an outgoing call; picking up a call from Manual Hold; or Group pickup. Phone users include keyset users and mobile users logged on to the phone. The special tone is triggered if one of the following SIP response codes is received from the server: 606, 408 or 503.

For current changes or additions see *OpenStage_SIP_FAQ#List_of_error_codes* in the *Siemens Enterprise Wiki* under *http://wiki.siemens-enterprise.com/wiki*

5 Examples and HowTos

5.1 Canonical Dialing

5.1.1 Canonical Dialing Settings

The following example shows settings suitable for the conversion of given dial strings to canonical format. The example phone is located in Nottingham, UK.

Parameter	Example value	Explanation
Local country code	44	International country code for the UK.
National prefix digit	0	Used in front of national codes when dialed -without international prefix.
Local national code	115	Area code within the UK (here: Nottingham).
Minimum local number length	7	Minimum number of digits in a local PSTN number (e. g. 3335333 = 7 digits).
Local enterprise node	780	Prefix to access Nottingham numbers from within the Siemens network.
PSTN access code	9	Prefix to make an international call in the UK.
Operator codes	0,7800	Set of numbers to access the local operators. (No blank after comma, or else the subsequent entry is ignored.)
Emergency numbers	999,555	Set of numbers to access emergency services. (No blank after comma, or else the subsequent entry is ignored.)
Initial extension digits	2,3,4,5,6,8	1st digits of numbers that are used for extension numbers on the local node. (No blank after comma, or else the subsequent entry is ignored.)

5.1.2 Canonical Dial Lookup

The following example shows settings suitable for recognizing incoming numbers and assigning them to entries in the local phone book, and for generating correct dial strings from phone book entries, depending on whether the number is internal or external.

Parameter	Example value	Explanation
Local code <1>	780	Enterprise node prefix (here: Nottingham).
International code <1>	+44115943	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN (DID/DDI: direct inward dialing) is 943, which differs from the enterprise node prefix used within the enterprise network.
Local code <2>	722	Enterprise node prefix (here: Munich).
International code <2>	+4989722	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN for direct inward dialing is identical to the enterprise node prefix.

5.1.2.1 Conversion examples

In the following examples, numbers entered into the local phonebook by the user are converted according to the settings given above.

Example 1: Internal number, same node as the local phone

User entry		2345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+441159432345
Dial string sent when dialing from the phone book	Internal numbers = Local enterprise form	1234
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Example 2: Internal number, different node

User entry		7222345
External numbers		Local public form
External access code		Not required

International gateway code		Use national code
Number stored in the phone book		+49897222345
Dial string sent when dialing from the phone book	Internal numbers = Local enterprise form	2345
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Example 3: External number, same local national code as the local phone

User entry		011511234567
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+4411511234567
Dial string sent when dialing from the phone book	External numbers = Local public form	234567
	External numbers = National public form	011511234567
	External numbers = International form	004411511234567

5.2 An LLDP-Med Example

The following example illustrates the mode of operation of LLDP-MED. In order to evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port (see *LAN Port Settings*) is set to 100Mbit/s, hence a fixed value. This configuration error is detected and displayed by LLDP-MED. Please note the status of MAC_Phy config displayed in the local phone´s Admin menu.

Step by Step

1) Log in as administrator on the local phone´s **Admin** menu.

2) In the **Admin menu, navigate to Network > LLDP-MED Operation** using the navigation keys, and click **OK**.

3) In the LLDP-MED Operation submenu (see *LLDP-MED Operation*), navigate to MAC_Phy config and note the status displayed:

MAC_Phy config - Error

4) Select the **MAC_Phy config** submenu by pressing **OK** and navigate to the parameters displayed by using the navigation keys.

The following status is displayed for the **MAC_Phy config** parameters:

AutoSet enabled = Incompatible

MAU = Incompatible

5.3 Example Dial Plan

5.3.1 Introduction

A dial plan is a set of rules that determine the phone's behavior on digit entry by the user. Up to 48 rules are possible. With OpenScape Desk Phones, a dial plan rule is constructed from 9 parameters. In the following, the setup of a dial plan is explained.

The dial plan entries are preceded by a title line. This is a free format string, e. g. a descriptive name or version number, which can be used by the administrator for version control purposes.

5.3.2 Dial Plan Syntax

> ***INFO:*** The phone will not perform any checking on the title; ensuring that different dial plans are given different titles is part of the administration process.

A dial plan rule is built from the parameters described underneath.

- **Digit string**: A pattern of digits or "*", "#", or "x" characters that is to be matched for starting an action. The maximum length is 24 characters. The "x" character is a wildcard character that represents any of the other digits (it may be upper or lower case).
- **Action**: The action to be taken when the criteria are met. The following options are available:
  - "S" (Send digits): The digits entered are sent to the server when one of the following three conditions is satisfied:
    a) the maximum digits have been received, or
    b) the timer expires after the minimum digits have been received, or
    c) on receipt of the terminator after the minimum digits.
  - "C" (Check for other actions): If the digit sequence entered by the user matches **Digit string**, **Maximum length**, and **Minimum length**, the timer starts. On timer expiry, the digit string will be sent to the server. If further digits are received before timer expiry, further entries will be checked. If the timer is set to 0, the dial string will be sent immediately. This option is used when there are more than one rules which start with the same digits.

- **Minimum length**: The dial plan rule will not initiate the sending of digits until at least this number of digits have been entered. However, the digits will be sent after the delay configured in **User menu > Configuration > Outgoing calls > Autodial delay (seconds)**.
- **Maximum length**: Automatic sending will occur when this number of digits have been dialed. If not specified, then the digits will be sent when the timer expires, or a terminating character is entered.
- **Timer**: This indicates the timeout to be used for subsequent digit handling. If not specified, the default timer value is used (**User menu > Configuration > Outgoing calls > Autodial delay (seconds)**).
- **Terminating character**: A "*" or "#" character which indicates that the preceding digits should be considered complete, even though the maximum length may not be reached. However, the reach the minimum length must be reached by the string built from the digits entered and the terminating characters.
- **Special indication**:
  - "E" (Emergency): If this character is entered here, the digits matching this rule will be sent even if the phone is locked. The number will be dialed immediately even when immediate dialing is disabled, and the phone is on-hook.
  - "b" (bypass): The phone lock is bypassed. The number will be dialed immediately even when immediate dialing is disabled, if the phone is off-hook.
- **Comment**: A remark on this dial plan entry.
- **Terminator sent**: If set to true, the terminating character is sent to the server along with the dial string proper. If set to false, the dial string is sent without the terminating character.

5.3.3 How To Set Up And Deploy A Dial Plan

Prerequisites

- For creating and deploying a dial plan to an OpenScape Desk Phone, a working installation of the DLS (version V2R4 onwards) is required. This HowTo describes the creation of a simple dial plan for OpenScape Desk Phones by example. Unless otherwise stated, the actions described underneath are performed in the DLS.

Step by Step

1) Log on to the DLS with an account that has suitable rights for deploying a dial plan. For details, please refer to the Deployment Service Administration Manual.

2) Navigate to IP Devices > IP Phone Configuration > Features > "Dialplan" tab.

3) Check dial plan, if not checked already.

4) Enter a suitable dial plan ID.

5) Click on to create the first dial plan rule.

6) Enter the following data:

Parameter	Value	Description/Remarks
Digit string	3	This rule matches numbers beginning with 3. For instance, theses might be internal numbers.
Action	S	When all criteria are met, the number is sent to the server.
Minimum length	4	This rule matches numbers with a length of 4 digits.
Maximum length	4	
Timer	0	The specified **Action** will take place without delay when all other criteria are met.

Summary: This rule determines that digit strings which begin with 3 and have a length of 4 digits are sent to the server without delay after the last digit has been entered.

7) Click on to create the second dial plan rule.

8) Enter the following data:

Parameter	Value	Description/Remarks
Digit string	0	This rule matches numbers beginning with 0. In the USA, this number calls the operator.
Action	C	When **Minimum length**, **Maximum length**, and the length of the digit string entered by the user match, the Timer is started. When it expires, the digits are sent to the server. When another digit is entered before expiry, the next dial plan entry will come into operation.
Minimum length	1	This rule matches numbers with a length of 1 digits.
Maximum length	1	
Timer	1	The phone waits 1 second for further digits. If the user does not enter any further digits, the action specified in **Action** is initiated.

Summary: When 0 is entered as first digit, the phone will wait 1 second. After this, 0 will be sent to the server, which might result in a call to an operator, for instance. When further digits are entered during the 1 second time span, the next dial plan rule will take control.

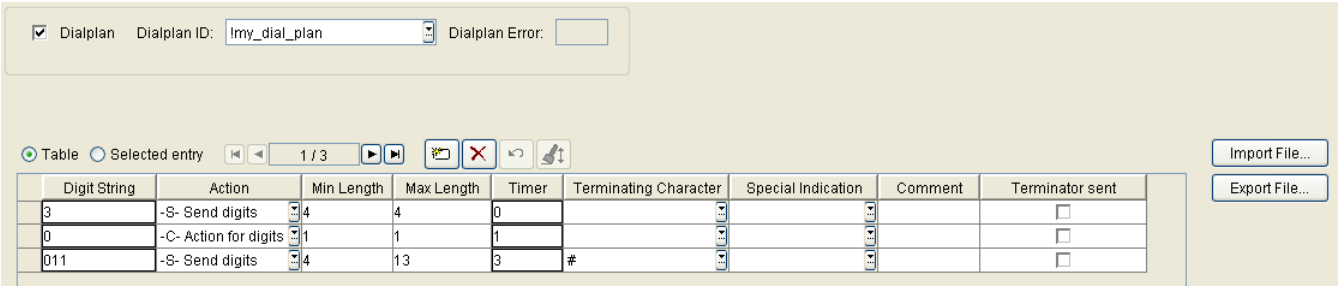
9) Click on to create the third dial plan rule.

10) Enter the following data:

Parameter	Value	Description/Remarks
Digit string	011	This rule matches numbers beginning with 011. In the USA, this digit string is the prefix international calls.
Action	S	When the entered digit string reaches the **Minimum length**, the **Timer** is started. On expiry, the digit string is sent.
Minimum length	4	When the length of the digit sequence entered by the user reaches this value, the Timer is started.
Maximum length	13	When the length of the digit sequence entered by the user reaches this value, the digits are sent to the server immediately. The **Timer** is overridden.
Timer	3	When the length of the digit sequence entered by the user reaches the **Minimum length**, the phone waits 3 seconds for further digits. If the user does not enter any further digits, the **Action** is triggered.
Terminating Character	#	When this character is entered, the digits are sent to the server immediately, regardless of the criteria contained in this rule.

Summary: Any numbers that start with 011 and have a length of 13 digits are sent to the server immediately. Shorter numbers with a length from 4 digits onwards are sent after a 3 seconds delay.

11) The example dial plan is completed; it should look like this:



12) You can check the dial plan using the phone's web interface; navigate to **Diagnostics > Fault trace configuration > Download dial plan file**.

6 Glossary

A

Address of Record (AoR)

A SIP URI that represents the "public address" of a SIP user resp. a phone or line. The format is similar to an E-mail address: "username@hostname".

ADPCM

Adaptive Differential Pulse Code Modulation. A compressed encoding method for audio signals which are to be transmitted by a low bandwidth. As opposed to regular PCM, a sample is coded as the difference between its predicted value and its real value. As this difference is usually smaller than the real, absolute value itself, a lesser number of bits can be used to encode it.

C

CSTA

Computer Supported Telecommunications Applications. An abstraction layer for telecommunications applications allowing for the interaction of CTI computer applications with telephony devices and networks.

CTI

Computer Telephony Integration. This term denotes the interaction of computer applications with telephony devices and networks.

D

DFT

Digital Feature Telephone. A phone with no line keys.

DHCP

Dynamic Host Configuration Protocol. Allows for the automatic configuration of network endpoints, like IP Phones and IP Clients.

DiffServ

Differentiated Services. Specifies a layer 3 mechanism for classifying and managing network traffic and providing quality of service (QoS) guarantees on IP networks. DiffServ can be used to provide low-latency, guaranteed service for e. g. voice or video communication.

DLS

The Deployment Service (DLS) is a HiPath management application for the administration of workpoints, i. e. IP Phones and IP Clients, in both HiPath- and non-HiPath networks.

DNS

Domain Name System. Performs the translation of network domain names and computer hostnames to IP addresses.

DTMF

Dual Tone Multi Frequency. A means of signaling between a phone and e. g. a voicemail facility. The signals can be transmitted either in-band, i. e. within the speech band, or out-band, i. e. in a separate signaling channel.

E

EAP

Extensible Authentication Protocol. An authentication framework that is frequently used in WLAN networks. It is defined in RFC 3748.

F

FTP

File Transfer Protocol. Used for transferring files in networks, e. g., to update telephone software.

G

G.711

ITU-T standard for audio encoding, used in ISDN and VoIP. It requires a 64 kBit/s bandwidth.

G.722

ITU-T standard for audio encoding using split band ADPCM. The audio bandwidth is 7 kHz at a sampling rate of 16 kHz. There are several transfer rates ranging from 32 to 64 kBit/s, which correspond to different compression degrees. The voice quality is very good.

G.729

ITU-T standard for audio encoding with low bandwidth requirements, mostly used in VoIP. The standard bitrate is 8 kBit/s. Music or tones such as DTMF or fax tones cannot be transported reliably with this codec.

Gateway

Mediation components between two different network types, e. g., IP network and ISDN network.

GUI

Graphical User Interface.

H

HTTP

Hypertext Transfer Protocol. A standard protocol for data transfer in IP networks.

I

IP

Internet Protocol. A data-oriented network layer protocol used for transferring data across a packet-switched internetwork. Within this network layer, reliability is not guaranteed.

IP address

The unique address of a terminal device in the network. It consists of four number blocks of 0 to 255 each, separated by a point.

J

Jitter

Latency fluctuations in the data transmission resulting in distorted sound.

L

LAN

Local Area Network. A computer network covering a local area, like an office, or group of buildings.

Layer 2

2nd layer (Data Link Layer) of the 7-layer OSI model for describing data transmission interfaces.

Layer 3

3rd layer (Network Layer) of the 7-layer OSI model for describing the data transmission interfaces.

LCD

Liquid Crystal Display. Display of numbers, text or graphics with the help of liquid crystal technology.

LDAP

Lightweight Directory Access Protocol. Simplified protocol for accessing standardized directory systems, e.g., a company telephone directory.

LED

Light Emitting Diode. Cold light illumination in different colors at low power consumption.

LLDP

Link Layer Discovery Protocol (IEEE Standard 802.1AB). Provides a solution for the discovery of elements on a data network and how they are connected to each other.

M

MAC Address

Media Access Control address. Unique 48-bit identifier attached to network adapters.

MDI-X

Media Dependent Interface crossover (X). The send and receive pins are inverted. This MDI allows the connection of two endpoints without using a crossover cable. When Auto MDI-X is available, the MDI can switch between regular MDI and MDI-X automatically, depending on the connected device.

MIB

Management Information Base. A type of database used to manage the devices in a communications network.

MWI

Message Waiting Indicator. A signal, typically a LED, to notify the user that new mailbox messages have arrived.

P

PBX

Private Branch Exchange. Private telephone system that connects the internal devices to each other and to the ISDN network.

PCM

Pulse Code Modulation. A digital representation of an analog signal, e. g. audio data, which consists of quantized samples taken in regular time intervals.

PING

Packet Internet Gro(u)per. A program to test whether a connection can be made to a defined IP target. Data is sent to the target and returned from there during the test.

PoE

Power over Ethernet. The IEEE 802.3af standard specifies how to supply power to compliant devices over Ethernet cabling (10/100Base-T).

Port

Ports are used in IP networks to permit several communication connections simultaneously. Different services often have different port numbers.

PSTN

Public Switched Telephone Network. The network of the world's public circuit-switched telephone networks.

Q

QoS

Quality of Service. The term refers to control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program. The OpenScape Desk Phone allows for the setting of QoS parameters on layer 2 and layer 3 (DiffServ).

QDC

QoS Data Collection. A HiPath IP service that is used to collect data from HiPath products in order to analyze their voice and network quality.

QCU

Quality of Service Data Collection Unit. A service tool that collects QoS report data from IP endpoints.

QoS

Quality of Service. Provides different priority to different users or data flows, or guarantee a certain level of performance to a data flow.

R

RAM

Random Access Memory. Memory with read / write access.

RTCP

Realtime Transport Control Protocol. Controls the RTP stream and provides information about the status of the transmission, like QoS parameters.

RTP

Realtime Transport Protocol. This application layer protocol has been designed for audio and video communication. Typically, the underlying protocol is UDP.

S

SDP

Session Description Protocol. Describes and initiates multimedia sessions, like web conferences. The informations provided by SDP can be processed by SIP.

SIP

Session Initiation Protocol. Signaling protocol for initialising and controlling sessions, used e. g. for VoIP calls.

SNMP

Simple Network Management Protocol. Used for monitoring, controlling, and administration of network and network devices.

SNTP

Simple Network Time Protocol. Used to synchronize the time of a terminal device with a timeserver.

Subnet Mask

To discern the network part from the host part of an IP address, a device performs an AND operation on the IP address and the network mask. The network classes A, B, and C each have a subnet mask that demasks the relevant bits: 255.0.0.0 for Class A, 255.255.0.0 for Class B and 255.255.255.0 for Class C. In a Class C network, for instance, 254 IP addresses are available.

Switch

Network device that connects multiple network segments and terminal devices. The forwarding of data packets is based on MAC addresses: data targeted to a specific device is directed to the switch port that device is attached to.

T

TCP

Transfer Control Protocol. The protocol belongs to the transport layer and establishes a connection between two entities on the application layer. It guarantees reliable and in-order delivery of data from sender to receiver, as opposed to UDP.

TLS

Transport Layer Security. Ensures privacy between communicating applications. Typically, the server is authenticated, but mutual authentication is also possible.

U

UDP

User Datagram Protocol. A minimal message-oriented transport layer protocol used especially in streaming media applications such as VoIP. Reliability and order of packet delivery are not guaranteed, as opposed to TCP, but UDP is faster and more efficient.

URI

Uniform Resource Identifier. A compact string of characters used to identify or name a resource.

URL

Uniform Resource Locator. A special type of URI which provides means of acting upon or obtaining a representation of the resource by describing its primary access mechanism or network location.

V

VLAN

Virtual Local Area Network. A method of creating several independent logical networks within a physical network. For example, an existing network can be separated into a data and a voice VLAN.

VoIP

Voice over IP. A term for the protocols and technologies enabling the routing of voice conversations over the internet or through any other IP-based network

W

WAP

Wireless Application Protocol. A collection of protocols and technologies aiming at enabling access to internet applications for wireless devices. WAP can also be used by the OpenScape Desk Phone.

WBM

Web Based Management. A web interface which enables configuration of the device using a standard web browser.

WML

Wireless Markup Language. An XML-based markup language which supports text, -graphics, hyperlinks and forms on a WAP browser.

WSP

Wireless Session Protocol. The protocol is a part of the WAP specification. Its task is to establish a session between the terminal device and the WAP gateway.

Index

T

U

V

W

Z